



Symantec™ Endpoint Protection 14.3 RU9 Installation and Administration Guide

Updated: June 25, 2024

Table of Contents

Release Notes.....	18
What's new for Symantec Endpoint Protection 14.3 RU9?.....	18
Known issues and workarounds for Symantec Endpoint Protection (SEP).....	22
Tested virtual installations and virtualization products.....	34
Where to get more information.....	35
How to file a feature request or create a Support case.....	36
What is Symantec Endpoint Protection?.....	37
Symantec Endpoint Protection features.....	37
Symantec Endpoint Protection architecture components.....	40
Getting Started.....	42
Quick Start for Symantec Endpoint Protection.....	46
Installing Symantec Endpoint Protection Manager.....	51
Configuring Symantec Endpoint Protection Manager after installation.....	52
Installing Symantec Endpoint Protection Manager with a custom configuration.....	53
Logging on to the Symantec Endpoint Protection Manager console.....	56
Activating or importing your Symantec Endpoint Protection product license.....	59
Purchasing Symantec Endpoint Protection licenses.....	62
External URLs required for Symantec Endpoint Protection (SEP).....	63
Installing Symantec Endpoint Protection clients with Save Package.....	63
Installing Symantec Endpoint Protection clients with Remote Push.....	65
Installing Symantec Endpoint Protection clients with Web Link and Email.....	67
Installing the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.....	68
About the Symantec Single Agent for Linux.....	70
SEP Linux Agent and DCS Agent upgrade paths to Symantec Single Agent for Linux.....	71
Getting started on the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.....	71
Symantec Single Agent for Linux use cases.....	73
About auto-compile for the Symantec Endpoint Protection client for Linux.....	73
Installing the Symantec Endpoint Protection client for Mac.....	74
About authorizing system extensions for Symantec Endpoint Protection for macOS 10.15 or later.....	75
Managing kernel extension authorization when deploying the Symantec Endpoint Protection client for Mac.....	75
What do I do after I install the management server?.....	76
Communication ports for Symantec Endpoint Protection.....	78
Installing and Uninstalling the Management Server and Clients.....	81
Network architecture considerations.....	81
About choosing a database type.....	82
About basic management server settings.....	82

About SQL Server configuration settings.....	83
About SQL Server database authentication modes.....	86
Internationalization requirements.....	88
Uninstalling Symantec Endpoint Protection.....	89
Configuring Symantec Endpoint Protection to be FIPS 140-2-compliant.....	91
Understanding Symantec Endpoint Protection and FIPS 140-2 level 1 compliance.....	93
Versions that support FIPS 140-2 level 1 compliance.....	94
Unsupported features and limitations in the FIPS 140-2 level 1-compliant mode.....	95
Enabling or disabling the FIPS mode for the Symantec Endpoint Protection Manager.....	95
Installing the SQL Server database certificate.....	96
About the FIPS-compliant libraries.....	99
About the validated modules.....	100
Troubleshooting FIPS 140-2 compliance issues on Symantec Endpoint Protection.....	101
Managing the Symantec Endpoint Protection client installation.....	101
Preparing Windows and Mac computers for remote deployment.....	103
Choosing a method to install the client using the Client Deployment Wizard.....	105
Choosing which security features to install on the client.....	105
Managing client installation packages.....	106
Exporting client installation packages.....	107
Importing client installation packages into Symantec Endpoint Protection Manager.....	108
Windows client installation package and content update sizes.....	109
Creating custom Windows client installation packages in Symantec Endpoint Protection Manager.....	110
About the Windows client installation settings.....	111
Customizing the client installation settings.....	111
Uninstalling existing third-party security software.....	112
Choosing whether to download cloud-based or local-based definitions using the client installation type.....	113
Third-party security software removal in Endpoint Protection/Endpoint Security.....	114
Third-party security software removal in Symantec Endpoint Security/Symantec Endpoint Protection 14.3 RU1 and later.....	114
Restarting the client computers from the Symantec Endpoint Protection Manager.....	117
About managed and unmanaged (self-managed) clients.....	118
How to get an unmanaged client installation package.....	119
Installing an unmanaged Windows client.....	120
About uninstalling the Symantec Endpoint Protection client.....	121
Uninstalling the Symantec Endpoint Protection client for Windows.....	122
Uninstalling the Symantec Endpoint Protection client for Mac.....	123
Uninstalling the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.....	123
Deleting a client.....	125
Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection (SEP).....	126
Upgrade best practices for Endpoint Protection 14.x.....	127

Upgrade resources for Symantec Endpoint Protection.....	131
Upgrading Windows client computers to 14.3 RU8 and later with Microsoft Azure Code Signing (ACS) support.....	131
Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection.....	136
Increasing Symantec Endpoint Protection Manager available disk space before an upgrade.....	137
Upgrading the management server.....	138
Best practices for upgrading from the embedded database to the Microsoft SQL Server Express database...	139
Reducing the database size when the database is full before an upgrade to Microsoft SQL Server Express...	141
Enabling FILESTREAM for the Microsoft SQL Server database.....	142
Reducing the database size to less than 10 GB before an upgrade to Microsoft SQL Server Express.....	143
Making more disk space available to upgrade to the default Microsoft SQL Server Express database.....	145
Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server.....	146
Symantec Endpoint Protection Manager has detected that the configured email server or directory server requires certificate verification to be disabled.....	159
Resolving Microsoft SQL Server database connection errors after 14.3 RU5 or later installation or upgrade...	162
Upgrading an environment that uses multiple embedded databases and management servers.....	169
Reconfiguring Symantec Endpoint Protection Manager after changing the computer's IP address and host name.....	169
Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate (14.3 RU9 or later).....	172
Symantec Endpoint Protection Manager detected that the configured replication partner requires host name verification to be disabled (14.3 RU9 or later).....	175
Troubleshooting: Your server certificate is not valid because the computer host name or IP address changed (14.3 RU8 or later).....	178
Stopping and starting the management server service.....	182
Preventing replication during an upgrade.....	183
Restoring replication.....	184
Choosing which method to upgrade the client software.....	185
Upgrading client software with AutoUpgrade.....	186
Applying AutoUpgrade settings to other groups.....	188
Upgrading client software with the Client Upgrade policy.....	189
Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language.....	191
Installing Endpoint Protection client patches on Windows clients.....	192
Upgrading the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.....	193
Updating the kernel modules for Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.....	194
Upgrading Group Update Providers.....	196
Migrating to the SES cloud console.....	197
Benefits of moving to the Symantec Endpoint Security cloud console.....	198
On-premises, hybrid, or fully cloud management options.....	199
Enrolling a Symantec Endpoint Protection Manager domain with the cloud server (14.3 RU3 or later).....	201

How do I manage clients and policies after I enroll a Symantec Endpoint Protection Manager domain with the cloud server?.....	205
How a hybrid-managed Symantec Endpoint Protection Manager (SEPM) interacts with the Symantec Endpoint Security (SES) cloud console.....	207
Differences in features between an on-premises SEPM and a cloud-enrolled SEPM.....	210
Troubleshooting communication issues between a hybrid Symantec Endpoint Protection Manager, clients, and the cloud server.....	214
Enabling Adaptive Protection in Symantec Endpoint Protection.....	216
Viewing Cloud Analytics incidents on Symantec Endpoint Protection Manager (14.3 RU8 and later).....	220
Troubleshooting issues on the Advanced Security page.....	222
How does the Symantec Endpoint Protection Manager Exceptions policy interact with the Symantec Endpoint Security (SES) cloud console?.....	224
Enrolling sites with replication partners in the cloud server.....	227
Updating clients in low-bandwidth environments.....	229
Monitoring roaming Symantec Endpoint Protection clients from the cloud console.....	231
Unenrolling Symantec Endpoint Protection Manager domains from the cloud server.....	232
Licensing Symantec Endpoint Protection.....	234
When does my Symantec Endpoint Protection license expire?.....	235
How do I receive a notification that my Symantec Endpoint Protection licenses are expiring?.....	236
What happens when a license expires or is overdeployed (SEP or SES)?.....	236
Make more licenses available by deleting obsolete licenses.....	240
What does a Symantec Endpoint Protection license cover?.....	241
Backing up and recovering your license file (.slf).....	242
About multi-year licenses.....	242
Symantec Endpoint Protection product license terminology.....	243
Licensing an unmanaged Windows client.....	243
Using Policies to Manage Security.....	245
Best practices for stopping malware and other threats.....	245
Ransomware mitigation and protection with Symantec Endpoint Protection.....	246
Ransomware protection using Symantec Endpoint Protection.....	248
What's new in ransomware protection against living-off-the land techniques (SEP and SES).....	251
How do I block websites with Symantec Endpoint Protection?.....	254
Performing the tasks that are common to all policies.....	255
The types of security policies.....	256
Updating security policies on the Windows client.....	258
Creating a custom Symantec Endpoint Protection Manager policy.....	258
Editing a policy.....	259
Finding a policy's default settings.....	259
Copying and pasting a policy on the Policies page.....	260
Copying and pasting a policy on the Clients page.....	260

Assigning a policy to a group or location.....	261
Replacing a policy.....	262
Exporting and importing individual Endpoint Protection policies.....	262
About shared and non-shared policies.....	263
Converting a shared policy to a non-shared policy.....	264
Unassigning a policy from a group or location.....	265
Enabling application learning.....	265
Searching for information about the learned applications that the computers run.....	267
Managing firewall protection.....	268
How a firewall works.....	269
About the Symantec Endpoint Protection firewall.....	269
Creating a firewall policy.....	270
Managing firewall rules from the Symantec Endpoint Protection Manager.....	272
Adding a new firewall rule.....	273
About firewall server rules and client rules.....	273
What is the order that the firewall processes the firewall rules and settings.....	275
About inherited firewall rules.....	275
Adding inherited firewall rules from a parent group.....	276
Changing the order of firewall rules.....	277
How the firewall uses stateful inspection.....	277
About firewall rule application triggers.....	278
About firewall rule host triggers.....	281
Adding host groups.....	282
About firewall rule network services triggers.....	283
Adding network services to the default network services list.....	283
About firewall rule network adapter triggers.....	284
Adding a custom network adapter to the network adapter list.....	284
Copying Symantec Endpoint Protection firewall rules.....	285
Customizing firewall rules.....	286
Configuring firewall settings for mixed control.....	293
Enabling communications for network services instead of adding a rule.....	294
Automatically blocking connections to an attacking computer.....	295
Detecting potential attacks and spoofing attempts.....	295
Preventing outside stealth attacks on computers.....	296
About firewall settings for the Mac client.....	297
Disabling the Windows Firewall.....	298
Configuring intrusion prevention.....	298
How intrusion prevention works.....	307
Enabling intrusion prevention.....	308

Integrating browser extensions with Symantec Endpoint Protection (SEP) to protect against malicious websites.....	308
Setting up a list of excluded computers.....	316
Configuring client notifications for intrusion prevention and Memory Exploit Mitigation.....	317
About Symantec IPS signatures.....	317
Creating exceptions for IPS signatures.....	318
Managing custom intrusion prevention signatures.....	319
About custom IPS signatures.....	320
Creating a custom IPS library.....	321
Adding signatures to a custom IPS library.....	321
Changing the order of custom IPS signatures.....	322
Defining variables for custom IPS signatures.....	323
Assigning multiple custom IPS libraries to a group.....	324
Testing custom IPS signatures.....	324
Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy.....	324
Symantec Endpoint Protection Memory Exploit Mitigation techniques.....	329
Preventing and handling virus and spyware attacks on client computers.....	330
Removing viruses and security risks.....	331
Identifying the infected and at-risk computers.....	333
Checking the scan action and rescanning the identified computers.....	333
How Windows clients receive definitions from the cloud.....	334
Managing scans on client computers.....	336
About the types of scans and real-time protection.....	337
About the types of Auto-Protect.....	339
About virus and security risks.....	341
About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans.....	342
About the default Virus and Spyware Protection policy scan settings.....	344
How Symantec Endpoint Protection handles detections of viruses and security risks.....	346
Setting up scheduled scans that run on Windows computers.....	347
Setting up scheduled scans that run on Mac computers.....	349
Setting up scheduled scans that run on Linux computers.....	349
Running on-demand scans on client computers.....	350
Adjusting scans to improve computer performance.....	351
Adjusting scans to increase protection on your client computers.....	353
Managing Download Insight detections.....	354
How Symantec Endpoint Protection uses Symantec Insight to make decisions about files.....	356
How does Symantec Endpoint Protection use advanced machine learning?.....	357
How does the emulator in Symantec Endpoint Protection detect and clean malware?.....	359
Managing the quarantine for Windows clients.....	360
Scanning the SEP client computer using custom YARA rules.....	362

Managing the virus and spyware notifications that appear on client computers.....	365
Managing early launch anti-malware (ELAM) detections.....	366
Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options.....	367
Configuring a site to use a private Insight server for reputation queries.....	368
Configuring clients to use Symantec EDR or private servers for reputation queries and submissions.....	369
Customizing virus and spyware scans.....	370
Customizing the virus and spyware scans that run on Mac computers.....	372
Customizing the virus and spyware scans that run on Linux computers.....	372
Customizing Auto-Protect for Windows clients.....	373
Customizing Auto-Protect for Mac clients.....	374
Customizing Auto-Protect for Linux clients.....	374
Customizing Auto-Protect for email scans on Windows computers.....	376
Customizing administrator-defined scans for clients that run on Windows computers.....	377
Customizing administrator-defined scans for clients that run on Mac computers.....	377
Customizing administrator-defined scans for clients that run on Linux computers.....	378
Randomizing scans to improve computer performance in virtualized environments on Windows clients.....	379
Modifying global scan settings.....	380
Modifying log handling and notification settings on Windows computers.....	380
Modifying log handling settings on Linux computers.....	381
Customizing Download Insight settings.....	381
Changing the action that Symantec Endpoint Protection takes when it makes a detection.....	382
Allowing users to pause or stop scans on Windows computers.....	383
Configuring Windows Security Center notifications to work with Symantec Endpoint Protection clients.....	384
Submitting Symantec Endpoint Protection telemetry to improve your security.....	385
Understanding server data collection and client submissions and their importance to the security of your network.....	393
Managing the pseudonymous or non-pseudonymous data that clients send to Symantec.....	395
How Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth.....	396
Specifying a proxy server for client submissions and other external communications.....	396
Managing Behavioral Analysis (SONAR).....	397
What is Behavioral Analysis (SONAR) in Symantec Endpoint Protection?.....	398
Handling and preventing behavioral analysis (SONAR) false positive detections.....	399
Adjusting SONAR settings on your client computers.....	400
Monitoring behavioral analysis (SONAR) detection results to check for false positives.....	401
Protecting Symantec Endpoint Protection processes and resources with Tamper Protection.....	402
Application control, system lockdown, and device control.....	402
Setting up application control.....	403
Enabling and testing default application rules.....	404
The structure of an Application Control and Device Control policy.....	405
Adding custom rules to Application Control.....	406

Best practices for adding application control rules.....	408
Best practices for choosing which condition to use for a rule.....	409
Testing application control rules.....	410
Configuring system lockdown.....	411
Creating a file fingerprint list.....	415
Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager.....	417
Best practices for importing file fingerprint lists for SEP 14.3 RU5 and later.....	417
Updating a file fingerprint list in Symantec Endpoint Protection Manager.....	418
Interaction between system lockdown and Symantec EDR deny list (blacklist) rules.....	419
Creating an application name list to import into the system lockdown configuration.....	420
Automatically update file fingerprint lists to allow or block for system lockdown.....	421
Creating an index.ini file for automatic updates of allow lists and deny lists that are used for system lockdown.....	422
Enabling automatic updates of allow lists and deny lists for system lockdown.....	423
Troubleshooting file fingerprint list certificate issues.....	423
Setting up and testing the system lockdown configuration before you enable system lockdown.....	424
Blocking or allowing devices using Device Control and Application Control.....	425
Adding Device Control policy rules to allow or block devices on client computers.....	433
Adding hardware devices to the Hardware Devices list.....	434
Obtaining a device vendor or model for Windows computers with DevViewer.....	434
Mac Device Control in Endpoint Protection.....	435
Obtaining a device vendor, model, or serial number for Mac devices with DeviceInfo.....	437
How Application Control works to block devices.....	437
Applying exceptions to scans in Symantec Endpoint Protection.....	438
Which Windows exceptions do I use for what type of scan?.....	439
Creating exceptions for Virus and Spyware scans.....	440
Excluding a file or a folder from scans.....	442
Excluding known risks from virus and spyware scans on Windows clients.....	444
Excluding file extensions from virus and spyware scans on Windows clients and Linux clients.....	444
Creating an application exception.....	445
Excluding a trusted web domain from scans on Windows clients.....	446
Creating a Tamper Protection exception on Windows clients.....	447
Creating an exception for an application that makes a DNS or host file change.....	448
Excluding a certificate from scans on Windows clients.....	448
Restricting the types of exceptions that users can configure on client computers.....	449
Creating exceptions from log events.....	449
Controlling Internet access with Web and Cloud Access Protection.....	451
What is Web and Cloud Access Protection?.....	453
Verifying that the Web and Cloud Access Protection tunnel method is enabled and connected on the Windows client.....	457

Testing Web and Cloud Access Protection policies in a browser.....	460
Configuring the WSS Agent Block Notification Service for Web and Cloud Access Protection.....	462
Migrating Web and Cloud Access Protection from the PAC file redirection method to the tunnel method.....	463
Troubleshooting Web and Cloud Access Protection.....	465
Managing Web and Cloud Access Protection for the Mac client.....	469
Web and Cloud Access Protection Settings.....	470
Testing Symantec Endpoint Protection Manager policies.....	473
Testing a Virus and Spyware Protection policy.....	473
Blocking a process from starting on client computers.....	474
Preventing users from writing to the registry on client computers.....	474
Preventing users from writing to a particular file.....	475
Adding and testing a rule that blocks a DLL.....	476
Adding and testing a rule that terminates a process.....	477
Testing a default IPS policy.....	477
Managing the client-server connection.....	478
Improving client and server performance.....	478
About server certificates.....	480
Accepting the self-signed server certificate for Symantec Endpoint Protection Manager.....	481
Updating the server certificate on the management server without breaking communications with the client.....	482
Updating or restoring a server certificate.....	483
Checking whether the client is connected to the management server and is protected.....	485
Symantec Endpoint Protection client status icons.....	486
Using the policy serial number to check client-server communication.....	487
Updating policies and content on the client using push mode or pull mode.....	487
How does the client computer and the management server communicate?.....	489
Replacing the client-server communications file on the client computer.....	491
Restoring client-server communication settings with the SylinkDrop tool.....	492
Restoring client-server communications with Communication Update Package Deployment.....	492
Exporting and importing the client-server communications file (Sylink.xml) manually.....	493
Importing client-server communication settings into the Linux client.....	494
IPv6 networking support.....	495
Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients.....	495
Finding an available port.....	496
Changing the HTTPS port for Apache for client communication.....	496
Enabling HTTPS client-server communications.....	497
Managing Groups, Clients, Administrators, Passwords, and Domains.....	499
Managing groups of clients.....	499
How you can structure groups.....	500
Adding a group.....	500

Synchronizing Active Directory groups with the Symantec Endpoint Protection Manager (SEPM).....	501
What are organizational units in Active Directory?.....	506
Connecting Symantec Endpoint Protection Manager to a directory server.....	507
Connecting to a directory server on a replicated site.....	508
Importing organizational units from a directory server.....	509
Disabling a group's inheritance.....	509
Blocking client computers from being added to groups.....	510
Moving a client computer to another group.....	510
Managing client computers.....	511
Viewing the protection status of client computers.....	512
Enabling protection on the client computer.....	513
Searching for the clients that do not have the client software installed.....	513
Searching for information about client computers in the Symantec Endpoint Protection Manager.....	514
What are the commands that you can run on client computers?.....	515
Running commands on client computers from the console.....	516
Ensuring that a client does not restart.....	517
Switching a Windows client between user mode and computer mode.....	517
Configuring a client to detect unmanaged devices.....	518
Password-protecting the Symantec Endpoint Protection client.....	519
Preventing users from disabling the Symantec Endpoint Protection client.....	520
Allowing users to change settings on the Symantec Endpoint Protection client user interface.....	522
Collecting user information.....	524
Checking on your Mac client using AppleScript scripts.....	525
Managing your Linux client using the command line tool (sav).....	526
Managing remote clients.....	528
Managing locations for remote clients.....	529
Enabling location awareness for a client.....	531
Adding a location to a group.....	531
Changing a default location.....	532
Setting up Scenario One location awareness conditions.....	532
Setting up Scenario Two location awareness conditions.....	534
Configuring communication settings for a location.....	535
About strengthening your security policies for remote clients.....	536
Best practices for Firewall policy settings for remote clients.....	536
About turning on notifications for remote clients.....	537
About monitoring remote clients from the management server.....	537
Managing administrator accounts and passwords.....	538
About administrator accounts and access rights.....	539
Adding an administrator account and setting access rights.....	541
Choosing the authentication method for administrator accounts.....	541

Using RSA SecurID authentication with Symantec Endpoint Protection Manager.....	542
Configuring two-factor authentication with Symantec VIP.....	544
Configuring authentication with smart cards.....	545
Testing directory server authentication for an administrator account.....	550
Configuring Okta for the LDAP server with multifactor authentication (14.3 RU8 or later).....	553
Resetting a forgotten Symantec Endpoint Protection Manager password.....	554
Displaying the Forgot your password link so that administrators can reset lost passwords.....	556
Account name and password requirements for Symantec Endpoint Protection Manager.....	556
Changing the password for an administrator account or the default database.....	558
Enforcing a secure password for administrators and client users.....	559
Enabling Symantec Endpoint Protection Manager logon passwords to never expire.....	560
Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console.....	561
Displaying the Remember my user name and Remember my password check boxes on the logon screen.....	561
Granting or blocking access to remote Symantec Endpoint Protection Manager consoles.....	562
Unlocking an administrator account after too many logon attempts.....	563
Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console.....	564
About domains.....	565
Adding a domain.....	566
Switching to the current domain.....	567
How to update content and definitions on the clients.....	568
Choose a distribution method to update content on clients.....	569
Choose a distribution method to update content on clients based on the platform.....	574
Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager.....	574
Checking that Symantec Endpoint Protection Manager has the latest content.....	577
About the types of content that LiveUpdate downloads.....	578
Configuring clients to download content from an internal LiveUpdate server.....	582
Configuring clients to download content from an external LiveUpdate server.....	584
Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate.....	584
Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server.....	585
Configuring the LiveUpdate download schedule to client computers.....	585
Configuring the amount of control that users have over LiveUpdate.....	587
Mitigating network overloads for client update requests.....	587
About randomization of simultaneous content downloads.....	588
Randomizing content downloads from the default management server or a Group Update Provider.....	588
Reducing network congestion due to synchronous SEP client LiveUpdate content downloads.....	589
Configuring Windows client updates to run when client computers are idle.....	590
Configuring Windows client updates to run when definitions are old or the computer has been disconnected.....	590

Configuring clients to download content from the Symantec Endpoint Protection Manager.....	591
Testing engine updates before they release on Windows clients.....	591
Verifying which engine and definitions run on the client computers.....	594
Reverting to an older version of the Symantec Endpoint Protection security updates.....	595
Using Group Update Providers to distribute content to clients.....	596
About the types of Group Update Providers.....	597
Configuring Windows clients to download content from Group Update Providers.....	598
Searching for the clients that act as Group Update Providers.....	599
Configuring multiple types of Group Update Providers in your network.....	600
Using Intelligent Updater files to update content on Symantec Endpoint Protection clients.....	601
Using third-party distribution tools to update client computers.....	602
Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients.....	603
Preparing unmanaged clients to receive updates from third-party distribution tools.....	603
Distributing the content using third-party distribution tools.....	604
Monitoring, Reporting, and Enforcing Compliance.....	607
Configuring Host Integrity.....	607
How Host Integrity works.....	608
About Host Integrity requirements.....	610
Adding predefined requirements to a Host Integrity policy.....	611
Setting up remediation for a predefined Host Integrity requirement.....	612
Allowing users to delay or cancel Host Integrity remediation.....	612
Configuring the frequency of Host Integrity check settings.....	613
Allowing the Host Integrity check to pass if a requirement fails.....	614
Configuring notifications for Host Integrity checks.....	614
Creating a Quarantine policy for a failed Host Integrity check.....	615
Generating a list of computers where a Host Integrity check failed.....	615
Blocking a remote computer by configuring peer-to-peer authentication.....	616
Creating Host Integrity policy requirements by importing templates.....	617
Writing a customized requirement script.....	617
About registry conditions.....	618
Writing a custom requirement to run a script on the client.....	619
Writing a custom requirement to set the timestamp of a file.....	620
Writing a custom requirement to increment a registry DWORD value.....	621
Creating a test Host Integrity policy with a custom requirement script.....	621
Monitoring the Symantec Endpoint Protection clients.....	622
Finding unscanned computers.....	625
Finding offline computers.....	625
Generating a list of the Symantec Endpoint Protection versions installed in your network.....	625
Running a report on the deployment status of clients.....	626
Viewing risks.....	626

Viewing attack targets and sources.....	627
Viewing Symantec Endpoint Protection reports.....	627
Viewing system protection.....	628
Configuring reporting preferences.....	628
Logging on to reporting from a standalone web browser.....	629
About the types of Symantec Endpoint Protection Manager reports.....	630
Running and customizing quick reports.....	636
Saving custom reports.....	637
How to run scheduled reports.....	638
Editing the filter used for a scheduled report.....	639
Printing and saving a copy of a report.....	640
Viewing logs.....	640
About the types of Symantec Endpoint Protection Manager logs.....	641
Saving and deleting custom logs by using filters.....	643
Viewing logs from other sites.....	644
Exporting data to a Syslog server.....	644
Exporting log data to a text file.....	645
Configuring a failover server for external logging.....	646
Managing notifications.....	647
How notifications work.....	647
What are the types of notifications and when are they sent?.....	648
About partner notifications.....	650
Establishing communication between the management server and email servers.....	651
Viewing and acknowledging notifications.....	651
Saving and deleting administrative notification filters.....	652
Setting up administrator notifications.....	653
How upgrades from another version affect notification conditions.....	654
Managing management servers, sites, and databases.....	656
About the types of Symantec Endpoint Protection servers.....	656
Exporting and importing server settings.....	656
Managing Symantec Endpoint Protection Manager servers and third-party servers.....	657
Maintaining the database.....	658
Running automatic database backups.....	661
Scheduling automatic database maintenance tasks.....	661
Increasing the Microsoft SQL Server database file size.....	662
Specifying client log size and which logs to upload to the management server.....	662
Specifying the log size and how long to keep log entries in the database.....	663
About increasing the disk space on the server for client log data.....	663
Clearing log data from the database manually.....	664
Setting up failover and load balancing.....	664

About failover and load balancing.....	665
Configuring a management server list for load balancing.....	667
Installing a management server for failover or load balancing.....	668
Assigning a management server list to a group and location.....	669
Replacing a management server list.....	669
Setting up sites and replication.....	670
What are sites and how does replication work?.....	671
How to resolve data conflicts between sites during replication.....	673
Deciding whether or not to set up multiple sites and replication.....	674
Determining how many sites you need.....	675
How to install a second site for replication.....	676
Changing the replication frequency and content.....	677
Replicating data immediately.....	678
Deleting sites.....	678
Disaster recovery best practices for Endpoint Protection.....	679
Backing up the database and logs.....	680
Backing up a server certificate.....	681
Reinstalling or reconfiguring Symantec Endpoint Protection Manager.....	682
Generating a new server certificate.....	682
Restoring the database.....	683
Virtual environments with Symantec Endpoint Protection.....	685
About Shared Insight Cache.....	685
About the Virtual Image Exception tool.....	686
What do I need to do to use a network-based Shared Insight Cache?.....	686
System requirements for implementing a network-based Shared Insight Cache.....	687
Installing and uninstalling a network-based Shared Insight Cache.....	687
Enabling the use of a network-based Shared Insight Cache.....	688
Customizing Shared Insight Cache settings.....	689
About stopping and starting the network-based Shared Insight Cache service.....	692
Viewing network-based Shared Insight Cache log events.....	692
Monitoring network-based Shared Insight Cache performance counters.....	693
Troubleshooting issues with Shared Insight Cache.....	694
Using the Virtual Image Exception tool on a base image.....	694
System requirements for the Virtual Image Exception tool.....	695
Running the Virtual Image Exception tool.....	695
Configuring Symantec Endpoint Protection to bypass the scanning of base image files.....	696
Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures (NPVDIs).....	696
Setting up the base image for non-persistent guest virtual machines in non-persistent VDIs (NPVDIs).....	697
Purging obsolete non-persistent (NPVDI) clients to free up licenses.....	697
How to manage the license count for non-persistent virtual desktop infrastructure (NPVDI) clients.....	698

vietsol.....	699
vietsol.....	699
Troubleshooting Symantec Endpoint Protection.....	700
Troubleshooting and checking the health of the Windows client with SymDiag.....	701
Enabling TLS 1.0 and 1.1 on Microsoft Windows Server 2008 R2 during an installation or upgrade.....	702
Identifying the point of failure of a client installation.....	704
Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client.....	704
Checking the connection to the management server on the client computer.....	705
Investigating protection problems using the troubleshooting file on the client.....	706
Enabling and viewing the Access log to check whether the client connects to the management server.....	706
Stopping and starting the Apache Web server.....	707
Using the ping command to test the connectivity to the management server.....	707
Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client.....	707
Checking the debug log on the client computer.....	708
Checking the inbox logs on the management server.....	708
Troubleshooting the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.....	709
Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the default database.....	709
Verifying the management server connection with the database.....	710
Client and server communication files.....	712
Troubleshooting reporting issues.....	712
Changing timeout parameters for reviewing reports and logs.....	713
Accessing reporting pages when the use of loopback addresses is disabled.....	714
What you should know before you run Symantec Power Eraser from the Symantec Endpoint Protection Manager console.....	715
Tasks to perform when you must run Power Eraser from the Symantec Endpoint Protection Manager console.....	717
Starting Power Eraser analysis from Symantec Endpoint Protection Manager.....	720
Responding to Power Eraser detections.....	721
Appendices.....	723
Symantec Endpoint Protection features based on platform.....	723
Symantec Endpoint Protection feature dependencies for Windows clients.....	732
Tools that are included with Symantec Endpoint Protection.....	734
Commands for the Windows client service smc in Symantec Endpoint Protection and Symantec Endpoint Security.....	739
smc.exe command error codes.....	744
Installing Windows client software using third-party tools.....	745
About client installation features and properties.....	746
About configuring MSI command strings.....	746

About configuring Setaid.ini.....	746
Symantec Endpoint Protection command-line client installation properties.....	747
Installing Symantec Endpoint Protection client features using the command line.....	748
Windows Installer parameters.....	749
Windows Security Center properties.....	750
Command-line examples for installing the Windows client.....	751
Installing Windows clients with Microsoft SCCM/SMS.....	751
Installing Windows clients with an Active Directory Group Policy Object (GPO).....	752
Creating a GPO software distribution.....	753
Adding computers to an organizational unit to install software.....	754
Copying a Sylink.xml file to make a managed installation package.....	755
Uninstalling client software with an Active Directory Group Policy Object.....	755
Quick Start Guide for Symantec™ Endpoint Protection for Amazon Web Services.....	756
Documentation Legal Notice.....	759

Release Notes

Includes the [system requirements](#), supported upgrade paths, known issues, and links to more information.

Review the release notes before you install or upgrade Symantec Endpoint Protection, or contact Technical Support. The release notes include installation changes, upgrade issues, and known issues and workarounds.

What's new for Symantec Endpoint Protection 14.3 RU9?

These sections describe the new features in this release.

Symantec Endpoint Protection Manager

- The **Enable Browser Intrusion Prevention for Windows** option in the Intrusion Prevention policy automatically loads the Google Chrome and Microsoft Edge browser extensions for Symantec Endpoint Protection. However, this option overrides third-party extensions that organizations install if they use a different management tool. 14.3 RU9 provides an option that allows you to install and manage the extension with your tool of choice, such as Chrome Browser Cloud Management or Microsoft Intune.

To access this option, go to an Intrusion Prevention policy and make sure that the **Enable Browser Intrusion Prevention for Windows** option is selected and that the **Enable third-party management of extensions** option is cleared.

See: [Integrating browser extensions with Symantec Endpoint Protection \(SEP\) to protect against malicious websites](#)

- Fixed the following issues when Symantec Endpoint Protection Manager uses public CA-signed certificates as a result of adding Transport Layer Security (TLS) host name validation in 14.3 RU8:

- The Symantec Endpoint Protection Manager installation and upgrade requires that the management server name must also match one or more of the Subject Alternate Names (SANs) that are listed in the server certificate. In addition, the server name must use a valid host name, fully qualified domain name (FQDN), or IP address. If the server name and the SAN do not match, you must rename the server before you can continue.

See: [Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate \(14.3 RU9 or later\)](#)

- If Symantec Endpoint Protection Manager detects that the replication partner host name or IP address does not match one or more of the SANs for Symantec Endpoint Protection Manager, Symantec Endpoint Protection Manager allows the upgrade. After the upgrade, you can reenabling verification for increased security.

To access this option, right-click the replication partner site, click **Edit Replication Partner Properties**, and clear the **Disable verification of the partner server hostname** option.

To fix this issue, see: [Symantec Endpoint Protection Manager detected that the configured replication partner requires certificate verification to be disabled \(14.3 RU9 or later\)](#)

- When you log on to the Symantec Endpoint Protection Manager, you may see the following message about server certificates:

The server certificate could not be validated.

This message was in earlier releases, but provides additional information about why you see this error, including: You changed the computer hostname or IP address, or updated the server certificate recently. You need to use a valid hostname or IP address that matches your server certificate to log on to the Symantec Endpoint Protection Manager.

To fix this issue, see: [Error: Your server certificate is not valid because the computer host name or IP address changed \(14.3 RU8 or later\)](#)

- In earlier releases, to block the Symantec Endpoint Protection Manager from uploading file submissions, you had to configure your firewall to block the file submission URLs. 14.3 RU9 lets you allow or block file submissions through

the **Suspicious files pseudonymously to Symantec to enhance threat protection intelligence** option, which is allowed by default.

To access this option, go to **Clients > Policies tab > External Communications > Submissions tab > More options**.

- Improved the following hybrid management issues:

- In large organizations with multi-site replication between Symantec Endpoint Protection Manager and the cloud server, the synchronization may not occur correctly. The cloud sometimes underreports the number of groups or clients. In 14.3 RU9, before you migrate groups from the Symantec Endpoint Protection Manager using the **Switch Group to Cloud Managed** command, you can resynchronize the group hierarchy by running the

```
ASSET_SYNC_RESET
```

command. You can use this command to resynchronize up to 5,000 clients.

To view the event after you run the command, go to **Monitors > Log tab > System log type > Server Activity** content type. The following message appears:

The Symantec Endpoint Protection Bridge Service asset collector was reset successfully. All

- Symantec Endpoint Protection Manager now displays the following event when cloud unenrollment is successful but the API call to the cloud server fails:

Cloud unenrollment was successful on Symantec Endpoint Protection Manager but unsuccessful i
Integration page to remove all the data.

To access these log events, go to **Monitors > Log tab > System log type > Server Activity** content type.

To unroll the management server from the cloud console, see: [Enrolling and unenrolling Symantec Endpoint Protection Manager domains from the cloud server](#)

- The cloud connector uploads data successfully after the proxy configuration changes.
- Reduced unnecessary traffic to the cloud server on the operational state of the client.
- Improved data collection for environments with multi-site replication.
- Improved consistency of data between the Symantec Endpoint Protection Manager and the cloud console.
- Clarified the description of how the management server sends data if it is enrolled in the cloud console.

Go to the **Admin** page > **Servers > Site Properties** page > **General** tab. The following figure displays the description that you see above the **Move Up** and **Move Down** buttons.

Site Properties for Local Site (Site [redacted])

General LiveUpdate Passwords Data Collection Private Insight Server

Site Settings

Site Name: Site [redacted]

Description: [redacted]

Console Timeout: 1 hour

☐ Keep track of every application that the clients run

☐ Delete learned application data after: 30 days

The management console uses the first management server in the list to send reports and notifications. If the management server is enrolled in the cloud, it sends data to the cloud server. If a server is not available, the console uses the next server in the list. You can change the priority of servers by using the Move Up and Move Down buttons.

[redacted] Move Up Move Down

See: [Site Properties: General](#)

- Reporting includes the following enhancements:
 - You can configure secure communication (TLS) to the Syslog server.
You can access this option on the **External Logging** dialog box > **General** tab. In the **Destination Port** drop-down list, select **TLS**.

External Logging for Local Site (Site: [redacted])

General Log Filter

Send logs to a Syslog Server or export to a file.

Update Frequency: 30 seconds Primary Logging Server: [redacted]

☒ Enable Transmission of Logs to a Syslog Server

Syslog Server: [redacted]

Destination Port: TLS 6666

Log Facility: UDP TCP TLS

Log Line Separator: [redacted]

See: [Exporting data to a Syslog server](#)

- The Syslog report includes a **Correlation ID** field for the TAA incident ID.
- The newly added **14.3 RU5 and later** Client Install Feature Set no longer requires SONAR Protection (Behavioral Analysis) to be installed when Advanced Download Protection is installed.
To view this option, go to the **Admin** page > **Install Packages** > **Add Client Install Feature Set**, and then click the **Feature set version** drop-down list.

Add Client Install Feature Set

Name: [redacted]

Description: [redacted]

Feature sets for all previous versions are created automatically. You can also manually edit feature sets for previous versions.

Feature set version: 14.3 RU5 and later

☒ Virus, Spyware, and Basic Download Protection

☒ Advanced Download Protection

☐ Microsoft Outlook Scanner

☒ Proactive Threat Protection

☒ SONAR Protection

☒ Application and Device Control

Feature Description: Installs components for zero-day detection of viruses and spywares.

Required component(s):

See: [Choosing which security features to install on the client](#)

- The REST API supports the following commands:
 - To quickly add a large number of IP addresses and MAC addresses into a firewall rule, you can import a list of existing addresses into a host group, and then use a set of REST APIs that supports the GET, POST, and PUT methods for host groups.

See: [Symantec Endpoint Protection API commands](#)

- For compliance reporting, you can find update details for the IPS and Behavioral Analysis by using these REST API commands: GET /api/v1/computers returns ipsDefsetVersion and GET /api/v1/computers returns behavioralAnalysisDefsetVersion .
- The following third-party components were upgraded or added:
 - Apache Commons Codec
 - Apache Commons Compress
 - Apache Commons IO
 - Apache Commons Lang
 - Apache HTTP Server
 - Apache Tomcat
 - Apache Tomcat Native
 - curl
 - google guava
 - Jackson
 - JSON-java
 - libexpat
 - libssh2
 - libxml2
 - Nimbus JOSE+JWT
 - OpenJDK
 - OpenSC
 - OpenSSL
 - Spring Security
 - Spring Framework
 - zlib

Client and platform updates

Symantec Endpoint Protection Client for Windows

- To reduce the number of URLs that you must list in your proxy or perimeter firewall to communicate with the client, you only need to allow the following URLs.

Client management type	URLs to allow
All clients	• https://liveupdate.symantec.com • https://ent-shasta-rrs.symantec.com • https://sp.cwfservice.net
Cloud-managed clients	• https://us.spoc.securitycloud.symantec.com (North America) • https://eu.spoc.securitycloud.symantec.com (Europe) • https://in.spoc.securitycloud.symantec.com (India)

If you upgrade from 14.3 RU8 and earlier clients, you do not need to add or remove any URLs. Instead, the clients upgrade automatically after LiveUpdate next downloads content.

For information about all the URLs you need to allow, see: [External URLs required for Symantec Endpoint Protection \(SEP\) and Symantec Endpoint Security \(SES\)](#)

- The Windows client is supported on Windows 11 24H2.

Symantec Endpoint Protection Client for Mac

The Symantec Endpoint Protection Client for Mac releases in July 2024.

Symantec Single Agent for Linux

The Symantec Single Agent for Linux releases in July 2024.

Symantec Endpoint Security cloud console

The latest release of the cloud console provides the following enhancements for 14.3 RU9 clients:

- The Symantec Endpoint Security cloud console can send customized notifications to the client user after you manually quarantine a device.
- You can use the **Disable the notification area icon** option to prevent multiple instances of user session processes on the clients that run on a terminal server.
- Threat Defense for Active Directory (TDAD) includes updates such as the ability to cancel a running topology on the clients.

More information

- To learn more about the cloud-based features that are available with a Symantec Endpoint Security license, see: [What's new in Symantec Endpoint Security](#)
- To migrate to the cloud console, see: [Migrating to the SES cloud console](#)

Documentation

The documentation includes the following new topics:

- [Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate \(14.3 RU9 or later\)](#)
- [Symantec Endpoint Protection Manager detected that the configured replication partner requires certificate verification to be disabled \(14.3 RU9 or later\)](#)
- [How do I block websites with Endpoint Protection \(SEP\)?](#)
- [Blocking or allowing devices using Device Control and Application Control](#)
- [How Application Control works to block devices](#)
- [Deleting a client](#)

To view the database schema, contact Technical Support.

To find the open source attributions file, log on to the Broadcom portal and go to: [Symantec Endpoint Protection Open Source Attributions](#)

Known issues and workarounds for Symantec Endpoint Protection (SEP)

The items in this section apply to this release of Symantec Endpoint Protection.

NOTE

The Issue column displays the version number when the issue appears. For example, [14.3 RU1] means that the issue applies to version 14.3 RU1 and later. When these issues are fixed, they appear in the fix-it notes. See:

[Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security](#)

Known issues in 14.3 RU9

Table 1: Version 14.3 RU9

Issue ID	Description	Workaround
INFODEVSEP-70	The Symantec Endpoint Protection client 14.3 RU9 is incompatible with the on-premises Symantec EDR 4.9 and earlier. This issue is caused by the fewer number of URLs that you must allow for 14.3 RU9 clients. [14.3 RU9] External URLs required for Symantec Endpoint Protection (SEP) and Symantec Endpoint Security (SES)	This issue is fixed in Symantec EDR version 4.10, which is targeted to release in June 2024. If your environment includes Symantec EDR, do one of the following tasks: - Wait to upgrade to SEP 14.3 RU9 until Symantec EDR 4.10 is released and then upgrade them both at the same time. - Upgrade to SEP 14.3 RU9 at any time and install the Symantec EDR 4.9 patch.
INFODEVSEP-54	The following error message appears every 24 hours on the Admin > Servers page: The enrolled Symantec Endpoint Protection Manager did not replicate Adaptive Protection events with the remote site. [{_}sitename{_] } This issue occurs when the Symantec Endpoint Protection Manager is enrolled in the cloud console and has not replicated with its replication partner for at least two cycles. The replication partner usually does not replicate when the primary site is offline. [14.3 RU9]	You must successfully replicate between the sites.

[New fixes and component versions in Symantec Endpoint Protection 14.3 RU9](#)

Known issues in 14.3 RU8

Table 2: Version 14.3 RU8

Issue ID	Description	Workaround
SEP-85508	When using Live Shell in the client or cloud console, some text may be displayed incorrectly. Characters may be replaced with the Unicode replacement character (diamond with question mark) or other unexpected characters. [14.3 RU8 and earlier] See: Live Shell in ICDm displays a Unicode replacement character or other unintelligible characters	Upgrade to 14.3 RU9
ESMAC-7043	File Activity [8003] events are no longer sent by Mac agents connected to Symantec Endpoint Detection & Response (EDR). [14.3 RU8] For Mac agents reporting to the cloud console in Symantec Endpoint Security (SES), trigger a Full Dump to view 8003 events.	On-premise Mac agents configured to send events to EDR 4.8 and earlier will be enhanced in a future EDR release.

[New fixes and component versions in Symantec Endpoint Protection 14.3 RU8](#)

Known issues in 14.3 RU7

Table 3: Version 14.3 RU7

Issue ID	Description	Workaround
SEP-82895	After you restore a file that the SEP client quarantined, and then run an Auto-Protect scan on the restored file, the SEP client does not detect the virus. [14.3 RU7] This issue occurs when the Coexist with Windows Defender option is enabled and you restore a file from the quarantine. Windows Defender blocks Auto-Protect from detecting viruses in restored files, but can make its own detection.	1. Disable the Coexist with Windows Defender option. 2. Restore any files that have been in the quarantine and cleaned. 3. Reenable Coexist with Windows Defender.
SEP-82580	After disabling the Coexist with Windows Defender option within a Virus and Spyware Protection policy, Windows Defender is not disabled as expected. [14.3 RU7] When disabling co-exist mode, the Endpoint Protection/Security Agent is unable to disable Windows Defender if Windows Defender Tamper Protection is enabled because Windows Defender Tamper Protection blocks the action.	To allow the Endpoint Protection/Security agent to disable Windows Defender when disabling coexistence mode, Windows Defender Tamper Protection must be disabled. Alternatively, Windows Defender can be disabled manually. See: Windows Defender is not disabled when turning off coexistence mode in Endpoint Protection
SEP-83786	The Windows client Troubleshooting > Web and Cloud Access Protection page shows the following status message: Warning: Using CTCv1 (missing enrollment token) [14.3 RU7]	See: Warning: "Using CTCv1 (missing enrollment token)" warning in Web and Cloud Access Protection on SEP client 14.3 RU7 or later

[New fixes and component versions in Symantec Endpoint Protection 14.3 RU7](#)

Known issues in 14.3 RU6

Table 4: Version 14.3 RU6

Issue ID	Description	Workaround
SEPLINUX-1468	Monitoring of file system activity on the NFS file system is not yet supported for the EDR feature.	In 14.3 RU6 and later, only File rename and delete events are captured.
SEP-81247	If you remove the Advanced Download Protection feature from the Windows client, the SEPM still shows that the Advanced Download Protection feature is enabled. [14.3-RU6] Download Protection uses the IPS to retrieve information about files being accessed. If you remove Advanced Download Protection, you are not removing the IPS. Therefore, the Clients page > Clients tab still shows the Download Protection Status column as Enabled - Advanced Protection .	You can install the Basic Download Protection and Intrusion Prevention features, which are the same as Advanced Download Protection .

[New fixes and component versions in Symantec Endpoint Protection 14.3 RU6](#)

Known issues in 14.3 RU5

Table 5: Version 14.3 RU5

Issue ID	Description	Workaround
SEP-79993	When you upgrade from a 14.3 RU4 client to a 14.3 RU5 client and import a file fingerprint list that uses SHA-256 fingerprints, the system lockdown list does not correctly block applications. This issue occurs because the 14.3 RU5 and later client uses the 14.3 RU4 version of the <code>sysfer</code> and <code>sysplant</code> services.	Restart the 14.3 RU5 and later client after you upgrade from 14.3 RU4.
SEP-80222	The Status page on a 14.3 RU4 Windows client that a Symantec Endpoint Protection Manager 14.3 RU5 manages shows the following error: "Proactive Threat Protection is malfunctioning." [14.3 RU5]	The issue is caused because in 14.3 RU4 and earlier, SONAR depended on Auto-Protect being enabled. In 14.3 RU5, SONAR is no longer disabled when Auto-Protect is disabled. Therefore, when an 14.3 RU4 client receives the Virus and Spyware Protection policy from a Symantec Endpoint Protection Manager 14.3 RU5, SONAR is enabled but the client still shows the error. Security agents previous to 14.3 RU5 warn Proactive Threat Protection is not functioning when Auto-Protect is disabled by policy and locked
SEPLINUX-1502	In SEP 14.3 RU4 and earlier, when executing the forensic command to the Linux agent, the command would remain in the "In Progress" state for an extended period. [14.3 RU5]	The following are workarounds for this issue: 1. Cancel the command from the Symantec Endpoint Security (SES) console and re-issue it. 2. Allow the command to time out on the server. 3. Log on to the Agent system and restart the CAFDaemon.
SEPLINUX-1472	When running the Intelligent Updater script on RHEL9, a message appears on the console indicating that the "uncompress" executable is not present on the system. [14.3 RU5]	As of RHEL9, <code>ncompress</code> is deprecated. If you are running RHEL9, you must obtain <code>ncompress rpm</code> and install it on your system for the Intelligent Updater to work. Intelligent Updater is not supported on RHEL9

Known issues in 14.3 RU4

Table 6: Version 14.3 RU4

Issue ID	Description	Workaround
SEP-77602	Attack Surface Reduce Log - Hardening Logs size ignores policy setting and is always 5 MB or larger. [14.3 RU4] In Symantec Endpoint Protection (SEP) agent version 14.3 RU4, the Attack Surface Reduction log maximum size is 5 MB (5,120 kb), even though the Security and Risk Logs Maximum Size in Client Log settings is configured to less than 5,120 KB. If the value is larger than 5,120 KB, then it adheres to the value. This issue occurs because the Attack Surface Reduction log (ASRman.log) contains more events than other Security and Risk logs (such as avman.log, tddadman.log). So a larger default size is required to retain sufficient events.	The 5 MB minimum is a temporary measure until a configurable value for Attack Surface Reduction is added to the Client Log settings. Until then, the log will either be 5mb or match the value that is configured in the Security and Risk log (whichever is larger). Attack Surface Reduce Log - Hardening Logs size ignores policy setting and is always 5MB or larger
	Symantec Endpoint Protection (SEP) 14.3 RU4 and older clients show the message <code>Component is Malfunctioning</code> as their SONAR status if Auto-Protect is disabled. The clients that show this message are managed by a Symantec Endpoint Protection Manager version 14.3 RU5 or later. For 14.3 RU4 and later clients, SONAR is not completely malfunctioning when Auto-Protect is disabled, but there is some efficacy impact on the SONAR component when Auto-Protect is disabled.	Make sure that you keep Auto-Protect enabled.
SEPLINUX-1488	Intelligent Updater fails to restart AMD service on RHEL6. [14.3 RU4]	If you are running RHEL6, you must restart the <code>sisamdagent</code> service (service <code>sisamdagent</code> restart) after running the Intelligent Updater script.
SEPLINUX-483	Linux agent does not communicate with DCS server. [14.3 RU4] If you are running RHEL/OEL/CentOS 8.x with FIPS mode enabled in dual-managed mode with a DCS agent, the agent is unable to communicate with DCS Server.	Communication is restored when you disable FIPS and restart the system. Dual managed DCS and SEP Linux are not supported.

New fixes and components for Symantec Endpoint Protection 14.3 RU4

Known issues in 14.3 RU3

Table 7: Version 14.3 RU3

Issue ID	Description	Workaround
SEP-72814	Endpoint Protection (SEP) 14.2 RU1 MP1 and earlier clients do not honor the Upgrade Schedule settings in a Client Upgrade Policy. [14.3 RU3]	For more information, see: Endpoint Protection 14.3 RU1 MP1 and older clients not following Client Upgrade Policy
SEPM-433	When you click the Advanced Security page, a blank page may appear with the following error message: File or Directory Was Not Found - The requested file or directory could not be located. [14.3 RU3 with a Symantec Endpoint Security Complete license] If the Symantec Endpoint Protection Manager and the Data Center Security client are installed on the same computer, LiveUpdate is not able to display the Advanced Security page content, and you cannot enroll the SEPM in the cloud console.	Configure the DCS prevention policy: 1. In the Symantec Data Center Security (DCS) Server Manager console, open the Prevention policy that is applied to the DCS client. 2. Click Application Rules. 3. In the Application Rules panel, select the Symantec Endpoint Protection entry. 4. Click Edit. 5. Add the following rules: – Program path: %%-HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM\JavaLaunchTool\JavaEXE%% – Program path: %%-HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM\JavaLaunchTool\JavaW%% 6. Enter a rule name and description as SEPM console. 7. Keep the remaining fields of the rule blank. 8. Save the policy and apply it to the DCS client. 9. In a Run command, stop and restart the Symantec Endpoint Protection Manager services as follows: – net stop semsrv – net stop semapisrv – net stop semwebsrv – net stop semlaunchsrv – net start semsrv – net start semapisrv – net start semwebsrv – net start semlaunchsrv
	Endpoint Protection 14.3 RU3 Web and Cloud Access Protection log reports the Windows 10 operating system as Windows 11. [14.3 RU3] In the SEP client Web and Cloud Access Protection log, the log shows the operating system as Windows 10 when the client is installed on a Windows 11 device. On the client console, click Web and Cloud Access Protection > Options > View Logs.)	

Issue ID	Description	Workaround
SEP-75086	Microsoft Edge browser and the Google Chrome browser are not able to launch after the Validate image dependency integrity mitigation technique is applied to the Windows 10 or 11 operating system. [14.3 RU3] One of the mitigation techniques that Microsoft Edge uses to protect the Windows operating system is the Validate image dependency integrity technique. For Windows 10 or 11 computers that run the Symantec Endpoint Protection clients versions 14.2 RU2 MP1 or later, if this option is enabled, both Microsoft Edge and the Google Chrome web browsers do not launch.	To ensure that Microsoft Edge launches, disable the Validate image dependency integrity technique. For more information on mitigation techniques for Microsoft Edge, see: Customize exploit protection See also: Microsoft Edge and Google Chrome do not open if "Validate image dependence integrity" mitigation technique is applied and SEP 14.2 RU2 MP1 or later is installed
SEP-73327	You must restart the rebootless Windows client to obtain the latest EDR events. [14.3 RU3] To make more ETW events available in 14.3 RU3, you must restart the Symantec Endpoint Protection client. You must restart the client in the following situations: • If EDR is enabled and you update the client to RU3. • 14.3 RU3 is already installed and you enable or disable EDR. You must restart the client to enable or disable the newly added events.	See: A restart may be required to begin seeing some ETW events with EDR and SEP 14.3 RU3
SEP-74510	Unexpected server error when logging into Endpoint Protection Manager and clients are no longer communicating after a system time change. [14.3 RU3] If you set the system clock back to a previous date and/or time, the following error may occur: • After you log on to the Symantec Endpoint Protection Manager, an Unexpected Server Error appears. • The clients do not communicate with SEPM, which reports a 503 error.	• Manually restart the SEPM services. • Wait until the date/time on the system passes the original time on the system before you set it back.
ESMAC-3339	On Mac client, VNC/screen sharing connectivity is lost if Vulnerability Protections are disabled or enabled. [14.3 RU3] Issue is observed on MacOS 12 and MacOS 11.4 (ARM).	

[New fixes and components for Symantec Endpoint Protection 14.3 RU3](#)

Known issues in 14.3 RU2

Table 8: Version 14.3 RU2

Issue ID	Description	Workaround
SEP-72531	The following error message appears: Symantec Endpoint Protection version 14.3 RU2 for Win64bit is the latest package. You cannot delete it. [14.3 RU2]	You cannot delete the Client Install Package when packages from multiple builds appear in the Symantec Endpoint Protection Manager. As of 14.3 RU2, LiveUpdate can download multiple client installation packages with a different build number, which appear in the Admin page > Install Packages > Client Install Package table.
SEP-72490	AutoUpgrade fails if you use the Upgrade to English if currently installed language is unsupported option to upgrade clients with an unsupported language to English. [14.3 RU2] This issue is caused because the client language uses the language of the supported operating system (in this case, Japanese). AutoUpgrade expects to use the supported language and not English.	Try the AutoUpgrade again and turn off the Upgrade to English if currently installed language is unsupported option.
	When exporting a client installation package from a 14.3 RU2 Symantec Endpoint Protection Manager (SEPM), the following warning message appears: "The client installation package does not have content." [14.3 RU2]	This issue occurs when communication between the Symantec Endpoint Protection Manager and the console being used to export the package is disrupted. See: "The client installation package does not have content." warning when exporting an installation package from the Endpoint Protection Manager
SEP-72292	An error appears when importing the most recent client installation packages into an older version of Symantec Endpoint Protection Manager. [14.3 RU2]	Symantec Endpoint Protection 14.3 RU2 clients cannot be managed by a 14.3 RU1 MP1 or earlier Symantec Endpoint Protection Manager.
SEP-70385	After upgrading a Symantec Endpoint Protection Manager to 14.3 RU2, php-cgi.exe crashes with an error in the event viewer. [14.3 RU2] This issue occurs with the 17.4.1.1 version of the Microsoft ODBC Driver for SQL Server in 14.3 RU2 clients.	Download and install the 17.7.2 version of the Microsoft ODBC Driver for SQL Server on Windows. Release Notes for Microsoft ODBC Driver for SQL Server on Windows php-cgi.exe crash occurs on Endpoint Protection Manager after upgrading to 14.3 RU2
	If you upgrade the Symantec Endpoint Protection Manager from 14.3 RU1 to a later version, you may see the following notifications: The client computer has been renamed [14.3 RU2] If upgrading from Symantec Endpoint Protection Manager 14.3 RU1 or earlier to 14.3 RU2 or later, administrators may start receiving The client computer has been renamed notifications. This issue is applicable only to Mac clients.	"The client computer has been renamed" notifications may appear after upgrading to Symantec Endpoint Protection Manager 14.3 RU2
	Custom names may prevent the firewall policy from updating during an upgrade to 14.2 or later. [14.3 RU2] For an upgrade to Symantec Endpoint Protection 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if you changed some default names. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected.	If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add.

Issue ID	Description	Workaround
	Rosetta may block the Mac agent installation on Apple Silicon (M1) devices with the following error: "This version of Symantec Agent for Mac is not supported on Apple M1 chip." [14.3 RU2]	For more information, see: Rosetta may block the Mac client installation on Apple Silicon (M1) devices

Known issues in 14.3 RU1

Table 9: Version 14.3 RU1

Issue ID	Description	Workaround
SEP-67175	Some EDR events do not appear on the client. [14.3 RU1]	The Symantec Endpoint Protection client must run Windows 10 build 14393 or later to collect Symantec EDR Event Tracing for Windows (ETW) events.
SEP-68700	The Web and Cloud Access Protection feature has some limitations. [14.3 RU1] • The Symantec Cloud Secure Web Gateway (Cloud SWG) was delivered on IPv4 and not IPv6. • The tunnel redirection method: – Runs on Windows 10 x64 version 1703 and later (Semi-Annual Servicing Channel), Windows 11, SEP Mobile, and the Mac. [SEP-67927] – Does not support HVCI-enabled Windows 10 64-bit devices. [SEP-67648] – Redirects outbound traffic from the Symantec Endpoint Protection client to the Cloud SWG before it gets evaluated by either the client's firewall or the URL reputation rules. Instead, that traffic is evaluated against the WSS firewall and the URL rules. For example, if a SEP client firewall rule blocks google.com and a WSS rule allows google.com, the client allows users to access google.com. Inbound local traffic to the client is still processed by the Symantec Endpoint Protection firewall. [SEP-67488] – SAML authentication replaced the Captive Portal to authenticate users and groups on the Symantec Endpoint Protection client. – If a client computer connects to the WSS using the tunnel method and hosts virtual machines, each guest user must install the SSL certificate provided in the Cloud SWG portal. – Traffic for local network like your home directory or Active Directory authentication is not redirected. – Is not compatible with the Microsoft DirectAccess VPN.	
SEP-68965	Duplicate client enrollment entries after the upgrade from 14.2.x to 14.3 MP1 and later. [14.3 RU1] Upgrading the Symantec Endpoint Protection clients from 14.2.x to 14.3 MP1 and later creates duplicate agent enrollment entries for these clients on the Clients page in Symantec Endpoint Protection Manager.	There is no functional impact and you can continue working with the new entries for 14.3 RU1 clients. Symantec Endpoint Protection Manager removes older agent entries.

Issue ID	Description	Workaround
SEP-75205	When you upgrade from the default SEPM embedded database to a Microsoft SQL Server Express database, the following error may appear: The specified password does not meet strong password requirements. [14.3 RU1] This error occurs because the SQL Server Express password requirements use the Windows password requirements. If the default database password requirements are more stringent than what the default SEPM installation script uses, this error occurs.	See: While upgrading a SEPM embedded database to 14.3 RU1 the error "The specified password does not meet strong password requirements"
SEP-69125	A Symantec Endpoint Protection Manager in a dark network downloads old Client Intrusion Detection System (CIDS) content to new clients because LiveUpdate does not run during an upgrade. [14.3 RU1] When a 14.3 RU1 or later Symantec Endpoint Protection Manager cannot access either the Internet or a LiveUpdate Administrator (LUA) server, it keeps old, incompatible content in its cache. This old content is normally delivered to the new clients. To update the content in the management server's cache, you manually download certified virus definitions and CIDS .jdb files.	To make sure that the new clients do not get old content, manually install a CIDS .jdb file on SEPM before you install new clients or upgrade old clients. See: Download .jdb files to update definitions for Endpoint Protection Manager
	You cannot log on to Symantec Endpoint Protection Manager (SEPM) when the network interface card is disabled. [14.3 RU1] If after you install Symantec Endpoint Protection Manager, you cannot log on to the console and the following error message appears: <code>Unexpected server error</code> This issue may occur if the computer's network interface card is disabled when you installed the SEPM, which keeps the server certificate from being generated. This issue occurs when certificate validation fails during installation because the SEPM installer is unable to get the host name if all network cards are disabled. The . . . \apache\conf\server.crt file shows the Issued to and Issued by fields as blank.	Enable at least one network adapter, uninstall the SEPM, then reinstall the SEPM. See: Unexpected server error at SEPM login if it was installed on a server without an enabled NIC
SEP-68670	When you uninstall SEPM and use the option to remove the default database and leave the SQL Server Express instance, the following error appears: "An error occurred while trying to connect to the database server". [14.3 RU1] If you uninstall the Symantec Endpoint Protection Manager and select the Remove only the DB and leave the SQL Server Express instance installed with SEPM option, you may see the following error: "An error occurred while trying to connect to the database server." This issue occurs after you add the credentials for the default user DBA and may be related to user privileges.	Perform the uninstallation by running the SEPM setup.exe file and clicking the Remove only the DB and leave the SQL Server Express instance installed with SEPM option during uninstallation.
SEP-70996	Upgrade installation package that is used for clean installation installs the default feature set. [14.3 RU1 MP1 and earlier] If you create an upgrade installation package with Maintain existing client features when updating option checked, and use this package to do a clean installation, the default feature set is installed on your client device.	If you want to install a custom feature set, you must create a separate installation package for the clean installation.
SEP-72481	If you automatically upgrade a client with an unsupported language to English, the client continues to display the date settings for definitions in English. [14.3 RU1 and later]	Uninstall the legacy client and manually install a new English client installation package. In addition, a fix is expected for clients that are upgraded automatically.

Known issues in 14.3 and earlier

Table 10: Versions 14.3.x and earlier

Issue ID	Description	Workaround
SEP-61473	A SQL Server upgrade from version 2017 to version 2019 fails with FIPS mode enabled. [14.3] You may see the error: "The following error has occurred. An error occurred while installing the extensibility feature with the error message: AppContainer Creation Failed with error message NONE state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms." This issue occurs if you have a FIPS-enabled Symantec Endpoint Protection Manager 14.3 and you upgrade from the Microsoft SQL Server 2017 through 2019.	Disable FIPS at the operating system level: 1. In C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools, click Local Security Policy > Local Policies > Security Options, and disable System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing 2. Upgrade from SQL Server version 2017 to version 2019. 3. After SQL Server upgrades successfully, re-enable FIPS. For more information, see: SQL upgrade from 2017 to 2019 fails with FIPS mode enabled
SEP-61106	The Symantec Endpoint Protection Manager remote console no longer supports the 32-bit Windows platform. [14.3] In 14.3 and later, you cannot log on to the Symantec Endpoint Protection Manager remote console if you run a 32-bit version of Windows. The Oracle Java SE Runtime Environment no longer supports 32-bit versions of Microsoft Windows.	If you see the following message, log on to Symantec Endpoint Protection Manager locally: "This version of C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe is not compatible with the version of Windows that you are running. Check your computer's system information and then contact the software publisher."
SEP-60396	"Failed to install Microsoft Visual C++ Runtime" error appears while you install the Symantec Endpoint Protection Manager. [14.3] You may see the following error while installing the Symantec Endpoint Protection Manager on Windows 2012 R2: "Failed to install Microsoft Visual C++ Runtime"	To work around this issue, activate Windows and install the Windows updates. The Windows update installs the Visual C++ 2017 redistributable, which is a prerequisite for the Symantec Endpoint Protection Manager 14.3 installation on Windows 2012 R2.
	Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows. [14.3] After you upgrade to or install a Symantec Endpoint Protection Manager version 14.3 that is enrolled in the cloud console, the management server no longer uploads logs successfully to the cloud. In the uploader.log you may see the following error: <pre><SEVERE> WinHttpRequest: 12175: A security error occurred</pre>	This issue is caused by a missing Microsoft update that provides support for TLS 1.1 and 1.2. To solve the issue, install Microsoft update: KB3140245. For more information, see: Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows

Issue ID	Description	Workaround
	The standalone Symantec WSS Agent blocks the Symantec Endpoint Protection client installation if you install SEP on the same computer as the WSS Agent. The Web and Cloud Access Protection component uses the same files as the standalone Symantec WSS Agent (WSSA). Web and Cloud Access Protection is installed by default in both Symantec Endpoint Protection and the Symantec Endpoint Security cloud console. If Web and Cloud Access Protection is installed on an endpoint, WSSA cannot be installed. Similarly, if WSSA is installed, Web and Cloud Access Protection does not install.	You can remove the Web and Cloud Access Protection feature from existing endpoints without having to uninstall the whole client by using one of the following methods: - In Symantec Endpoint Protection Manager, create a Client Install Feature Set that does not include Web and Cloud Access Protection and apply it to the endpoints. See: Add or remove features to existing Endpoint Protection clients - The following command-line option uses the client installation file to remove Web and Cloud Access Protection: <code>setup.exe /s /v" REMOVE=NTR /qn"</code>
SEP-61175/61403	The Symantec Endpoint Protection 14.3 Windows client installation may fail unless you first install SHA-2 support. [14.3] If you run legacy operating system versions (Windows 7 RTM or SP1, Windows Server 2008 R2 or R2 SP1 or R2 SP2), you are required to have SHA-2 code signing support that is installed on your devices for Windows updates that are released on or after July 2019. Without SHA-2 support, the Windows client installation sometimes fails. The installation may fail whether you install clients for the first time or automatically upgrade from a previous release. If you want to run Windows Update on such machines you must pre-install the relevant patches too.	To get Microsoft enforced SHA-2 code signing support, see: 2019 SHA-2 Code Signing Support requirement for Windows and WSUS Symantec Endpoint Protection 14.3 Windows client may fail to install unless SHA-2 support is installed
CDM-42467	Allow URLs in Symantec Endpoint Security if you use the hybrid management option for a proxy server or a perimeter firewall. [14.3] With Broadcom's acquisition of Symantec Enterprise Security, the URLs for client-to-cloud communication changed in 14.2.2.1. This issue occurs when the Symantec Endpoint Protection Manager is enrolled in the Symantec Endpoint Security cloud console.	You must upgrade your clients to version build 14.3 MP1 (14.3.1169.0010) or later in the following situations. - You use Symantec Endpoint Security to manage your clients and policies when your on-premises Symantec Endpoint Protection Manager domains are enrolled in the cloud console. - You use proxy servers. You allow the URLs in either fully cloud-managed or hybrid-managed agents in your proxy server and/or perimeter firewall. See: External URLs required for Endpoint Protection (SEP) and Endpoint Protection (SES) Converting the Symantec Endpoint Protection clients from on-premises managed to cloud-managed

Issue ID	Description	Workaround
	"Deployment in progress" still appears in Symantec Endpoint Protection Manager after the client receives an updated policy for Endpoint Threat Defense for AD. [14.2 RU1 MP1 and later]	This behavior is expected. Endpoint Threat Defense for AD 3.3 policies are only supported on the client as of version 14.2 RU1 MP1. You apply a policy for Symantec Endpoint Threat Defense for Active Directory 3.3 to a group. This group contains some clients that run Symantec Endpoint Protection 14.2 RU1 or earlier. These clients receive and apply the policy as expected, but the status in the Symantec Endpoint Protection Manager continues to show the message Deployment in progress.
	Microsoft Edge unexpectedly allows PDF downloads with Hardening enabled. [14.2 RU1 MP1 and later] With Application Hardening enabled in the Symantec Endpoint Protection client, you are unexpectedly able to download PDF files if you use the Microsoft Edge browser. The prevention of the download of PDF files works as expected with other browsers.	A fix for this issue is planned for a future release.

[New fixes and components for Symantec Endpoint Protection 14.3 MP1](#)

[New fixes and components for Symantec Endpoint Protection 14.3](#)

Documentation

You can find documentation on the Broadcom [Symantec Security Tech Docs Portal](#).

To find the Endpoint Protection documentation, click the **Symantec Security Software** tab, then click **Endpoint Security and Management > Endpoint Protection**.

To find a PDF file, go to the [Related Documents](#) page.

To find the Symantec Endpoint Protection Manager database schema, contact Support.

Tested virtual installations and virtualization products

You can install Symantec Endpoint Protection on the tested operating systems that run in virtual environments. Install Symantec Endpoint Protection on the guest operating system, and not the host.

Symantec has tested the following virtualization products on the Symantec Endpoint Protection Manager, and the Symantec Endpoint Protection client software for Windows and Linux:

- Microsoft Azure
- Amazon Web Service (AWS) EC2
- Amazon WorkSpaces
- Citrix Studio Version 2009.0.0
- Nutanix AOS 5.15 (LTS)
- Oracle Cloud Infrastructure (OCI)
- Microsoft Virtual Server 2005
- Windows Server 2008 Hyper-V
- Windows Server 2008 R2 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V (As of 14.2 MP1)
- Windows Server 2019 Hyper-V Core Edition (As of 14.2 MP1)
- Citrix XenServer 5.6 or later
- Virtual Box, supplied by Oracle

NOTE

Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client do not interact directly with virtualization platforms such as [VMware ESX](#). That interaction is done between the operating system and the hypervisor. Make sure that both the Symantec Endpoint Protection Manager, client, and the chosen virtualization platform run on a supported operating system.

Symantec Endpoint Protection includes many features that enhance performance in virtual environments.

More information

- [Using Symantec Endpoint Protection Manager in virtual infrastructures](#)
- [Randomizing scans to improve computer performance in virtualized environments on Windows clients](#)
- For the most current system requirements, see: [Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security](#)

Where to get more information

The following table displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 11: Endpoint Protection website information

Types of information	Website link
Trial versions	Contact your account representative.
Manuals and documentation updates	Related Documents page For other languages, click the language drop-down menu.
Technical Support	Broadcom Technical Support Includes knowledge base articles, product release details, updates and patches, and contact options for support.
Threat information and updates	Symantec Security Center
Training	Education Services Access the training courses, the eLibrary, and more.
Symantec Connect forums	Endpoint Protection - Symantec Enterprise (broadcom.com)

How to file a feature request or create a Support case

To file a feature request or create a Support case for Symantec Endpoint Protection (SEP) or Symantec Endpoint Security (SES), see:

- [Open a Support case](#).
- Contact your [Broadcom partner](#). If you do not know your account manager, see the partner list.
- Call the [hotline](#) for your country.

Keep your Support Identifier or Contact ID available.

What is Symantec Endpoint Protection?

Learn about the Symantec Endpoint Protection architecture and components.

Symantec Endpoint Protection is a client-server solution that protects laptops, desktops, and servers in your network against malware, risks, and vulnerabilities. Symantec Endpoint Protection combines virus protection with advanced threat protection to proactively secure your client computers against known and unknown threats, such as viruses, worms, Trojan horses, and adware. Symantec Endpoint Protection provides protection against even the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks, and spyware that mutates.

Providing low maintenance and high power, Symantec Endpoint Protection communicates over your network to automatically safeguard both physical systems and virtual systems against attacks. Symantec Endpoint Protection provides management solutions that are efficient and easy to deploy and use.

More information

- [Symantec Endpoint Protection 14 datasheet](#)
- [How Symantec Endpoint Protection technologies protect your computers](#)
- [Symantec Endpoint Protection architecture components](#)

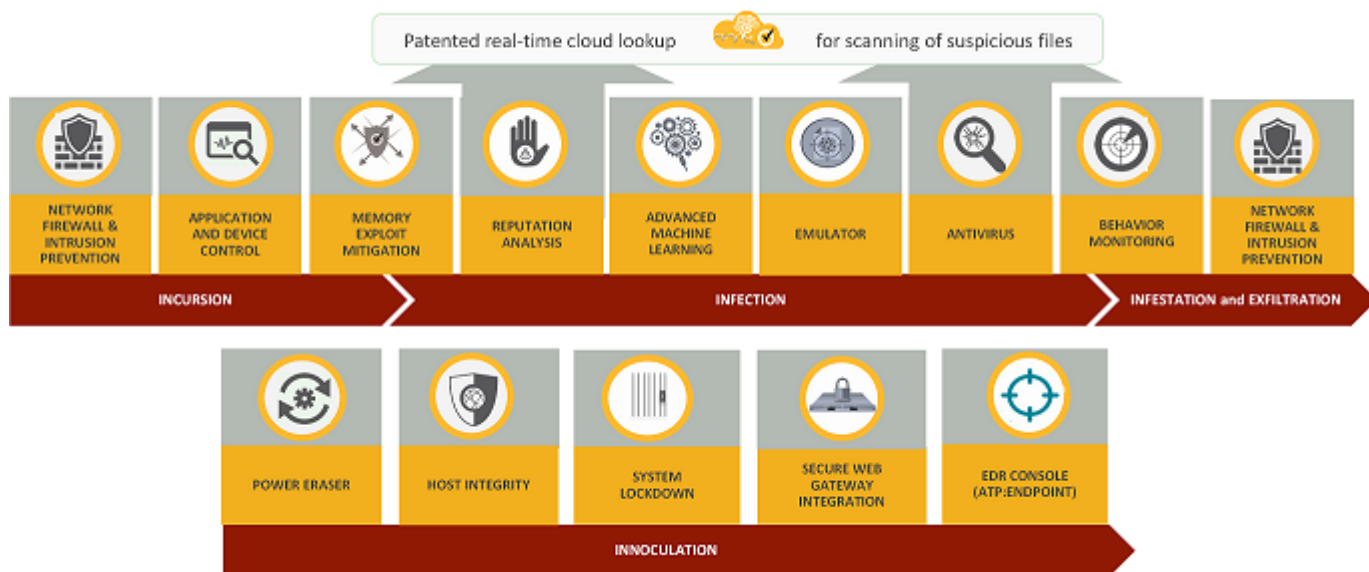
Symantec Endpoint Protection features

Symantec Endpoint Protection (SEP) uses the following core features to protect against known and unknown threats.

Symantec Endpoint Protection uses a layered approach to defense. The comprehensive approach protects the network before, during, and after an attack. Symantec Endpoint Protection reduces your risk of exposure by providing tools to increase your security posture ahead of any attack.

For the datasheet on Symantec Endpoint Protection, see: [Symantec Endpoint Protection 14](#)

To get complete protection for the computers in your network, enable all protections at all times.



For more information, see:

[What types of attacks do Symantec Endpoint Protection technologies protect against?](#)

Symantec Endpoint Protection uses the following holistic security approach to protect your environment across the entire attack chain, using the following stages: incursion, infection, infestation and exfiltration, and remediation and inoculation.

Phase 1: Incursion

During the incursion phase, hackers typically break into the organization's network using target attacks such as social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods.

Symantec Endpoint Protection protects against attacks before they enter your system using the following technologies:

- **Intrusion Prevention/Firewall (Network Threat Protection):** Analyzes all incoming traffic and outgoing traffic and offers browser protection to block such threats before they can be executed on the computer. The rules-based firewall and browser protection protect against web-based attacks. See:
 - [Managing intrusion prevention](#)
 - [Managing firewall protection](#)
- **Application Control:** Controls the file access and registry access and how processes are allowed to run. See:
 - [About application control, system lockdown, and device control](#)
 - [Setting up application control](#)
- **Device Control:** Restricts the access to select hardware and control what types of devices can upload or download information. See:
[Managing device control](#)
- **Memory Exploit Mitigation:** Neutralizes zero-day exploits like Heap Spray, SEHOP overwrite, and Java exploits in popular software that the vendor has not patched. See:
[Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)
- **Web and Cloud Access Protection:** Controls network traffic over all ports and protocols, regardless of where enterprise users are. See:
[Controlling Internet access with Web and Cloud Access Protection](#)

Phase 2: Infection

In targeted attacks, hackers typically break into the organization's network using social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods.

Symantec Endpoint Protection uses the following technologies to detect and prevent these attacks before they infect your system:

- **Memory Exploit Mitigation:** Detects malware.
- **File reputation analysis (Insight):** Based on the artificial intelligence that uses Symantec's global intelligence network. This advanced analysis examines billions of correlated linkages from users, websites, and files to identify and defend against rapidly-mutating malware. By analyzing key attributes (such as the origin point of a file download), Symantec can accurately identify whether a file is good or bad and assign a reputation score all before the file arrives on the client computer. See:
[Managing Download Insight detections](#)
- **Advanced machine learning:** Analyzes the trillions of examples of the good files and bad files that are contained in a global intelligence network. Advanced machine learning is a signatureless technology that can block new malware variants at the pre-execution. See:
[How does Symantec Endpoint Protection use advanced machine learning?](#)
- **High-speed emulation:** Detects hidden malware using polymorphic custom packers. A scanner runs each file in milliseconds in a lightweight virtual machine that causes threats to reveal themselves, improving both the detection rates and performance. See:
[How does the emulator in Symantec Endpoint Protection detect and clean malware?](#)
- **Antivirus file protection (Virus and Spyware Protection):** Uses signature-based antivirus and file heuristics to look for and eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits. See:

- [Managing scans on client computers](#)
- [About the types of scans and real-time protection](#)
- **Behavioral analysis (SONAR):** Leverages machine learning to provide zero-day protection, stopping new and unknown threats by monitoring nearly 1,400 file behaviors while they execute in real time to determine file risk. See: [Managing SONAR](#)

Phase 3: Infestation and Exfiltration

Data exfiltration is the unauthorized transfer of data from a computer. Once the intruders control these target systems, they may steal intellectual property or other confidential data. Attackers use captured information for analysis and further exploitation or fraud.

- **Intrusion Prevention/Firewall:** Block threats as they travel through the network.
- **Behavioral analysis:** Helps stop the spread of infection.

Phase 4: Remediation and Inoculation

Symantec Endpoint Protection includes a single console and agent that offers protection across operating systems, platforms, and businesses of any size.

- **Power Eraser:** An aggressive tool, which can be triggered remotely, to address advanced persistent threats and remedy tenacious malware. See: [What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console](#)
- **Host Integrity:** Ensures that endpoints are protected and compliant by enforcing policies, detecting unauthorized changes, and conducting damage assessments. Host Integrity then isolates a managed system that does not meet your requirements. See: [How Host Integrity works](#)
- **System Lockdown:** Allows applications (that are known to be good) to run, or blocks the applications (known to be bad) from running. In either mode, System Lockdown uses checksum and file location parameters to verify whether an application is approved or unapproved. System Lockdown is useful for kiosks where you want to run a single application only. See: [Configuring system lockdown](#)
- **Secure Web Gateway Integration:** Uses programmable REST APIs to make integration possible with Secure Web Gateway, to help quickly stop the spread of infection at the client computer.
- **EDR Console Integration.** Symantec Endpoint Protection is integrated with Symantec EDR and is designed to detect, respond, and block targeted attacks and advanced persistent threats faster by prioritizing attacks. EDR (Endpoint Detection and Response) capability is built into Symantec Endpoint Protection, which makes it unnecessary to deploy additional agents. See: [Configuring system lockdown](#)

What types of attacks do Symantec Endpoint Protection technologies protect against?

The following table displays which types of Symantec Endpoint Protection technologies protects against which types of attacks.

Table 12: What types of attacks does each Symantec Endpoint Protection technology protect against?

Attack	Advanced machine learning	Heuristics	Intrusion Prevention	Network Protection	Policy lockdown
Zero-day	√	√	√		√
Social engineering	√	√	√	√	√
Ransomware	√	√		√	√
Targeted attack	√	√	√		√

Attack	Advanced machine learning	Heuristics	Intrusion Prevention	Network Protection	Policy lockdown
Advanced persistent threat	√	√	√		
Drive-by download		√	√		

Symantec Endpoint Protection architecture components

The Symantec Endpoint Protection architecture uses three functional groups of components. Some of the components belong in multiple groups because they are multi-functional.



Table 13: Main components

Component	Description
Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager is a management server that manages events, policies, and client registration for the client computers that connect to your company's network. Symantec Endpoint Protection Manager includes the following subcomponents: - The management server software provides secure communication to and from the client computers and the console. - The console is the interface to the management server. The console software coordinates and manages security policies, client computers, reports, logs, roles and access, administrative functions, and security. You can also install a remote console and use it to log on to the management server from any computer with a network connection. - The database stores security policies and events and is installed with Symantec Endpoint Protection Manager. You can also install a Microsoft SQL Server database to use instead of the automatically installed Microsoft SQL Server Express (as of 14.3 RU1) or embedded database (14.3 MP1 and earlier). SQL Server is recommended for larger organizations with 5000+ computers. Symantec Endpoint Protection Manager communicates with either a local or remote Microsoft SQL Server database. For more information, see: Installing Symantec Endpoint Protection Manager
Symantec Endpoint Protection client	The Symantec Endpoint Protection client provides the security protection part of the solution. The client downloads policies and sometimes content from the Symantec Endpoint Protection Manager and runs on Windows, Mac, and Linux.

Symantec Endpoint Protection enables a client to download content from the management server, Group Update Provider, an Internal LiveUpdate server, or the Internet.

Table 14: Optional components and their functions

Component	Description
LiveUpdate Administrator	LiveUpdate Administrator downloads definitions, signatures, and other content from an internal LiveUpdate server and distributes the updates to client computers. You can use an internal LiveUpdate server in very large networks to reduce the load on the Symantec Endpoint Protection Manager. You should also use the internal LiveUpdate server if your organization runs multiple Symantec products that also use LiveUpdate to update client computers. For more information, see: • Download LiveUpdate Administrator (LUA) • Choose a distribution method to update content on clients • Configuring clients to download content from an internal LiveUpdate server
Group Update Provider (GUP)	The Group Update Provider helps distribute content within the organization, particularly useful for groups at remote locations with minimal bandwidth. Organizations that have a lot of clients may want to use Group Update Providers (GUPs) for Windows clients. GUPs reduce the load on the management server and are easier to set up than an internal LiveUpdate server. See: Using Group Update Providers to distribute content to clients
Symantec Endpoint Security (SES)	Symantec Endpoint Security is the cloud platform that you use to manage client computers from the cloud. Symantec Endpoint Security is the fully cloud-managed version of the on-premises Symantec Endpoint Protection. You can manage computers from any one of the following options: • Symantec Endpoint Protection Manager (on-premises only) • From Symantec Endpoint Protection Manager and Symantec Endpoint Security (hybrid: on-premises and cloud). See: Enrolling a domain in the cloud console from the Symantec Endpoint Protection Manager console • Symantec Endpoint Security (cloud only). See: Moving directly from a SEP on-premise option to a fully-cloud managed option On-premises, hybrid, or fully cloud management options

Symantec Endpoint Protection also comes with multiple tools to help you increase security and manage the product. For more information, see:

- [What are the tools included with Symantec Endpoint Protection?](#)
- [How Symantec Endpoint Protection technologies protect your computers](#)

Getting Started

Get up and running immediately on Symantec Endpoint Protection (SEP).

Assess your security requirements and decide if the default settings provide the balance of performance and security that you require. Some performance enhancements can be made immediately after you install Symantec Endpoint Protection Manager.

Perform the following tasks to install and protect the computers in your network immediately:

- [Step 1: Plan your installation structure](#)
- [Step 2: Prepare for and then install Symantec Endpoint Protection Manager](#)
- [Step 3: Add groups, policies, and locations](#)
- [Step 4: Change communication settings to increase performance](#)
- [Step 5: Activate the product license](#)
- [Step 6: Decide on a client deployment method](#)
- [Step 7: Prepare the client for installation](#)
- [Step 8: Deploy and install the client software](#)
- [Step 9: Check that the computers are listed in the groups that you expected and that the clients communicate with the management server](#)

For more information, see:

[What do I do after I install the management server?](#)

Step 1: Plan your installation structure

Before you install the product, consider the size and geographical distribution of your network to determine the installation architecture.

To ensure good network and database performance, you need to evaluate several factors. These factors include how many computers need protection, whether any of those computers connect over a wide-area network, or how often to schedule content updates.

- If your network is small, is located in one geographic location, and has fewer than 500 clients, you need to install only one Symantec Endpoint Protection Manager.
- If the network is very large, you can install additional sites with additional databases and configure them to share data with replication. To provide additional redundancy, you can install additional sites for failover or load balancing support. Failover and load balancing can only be used with Microsoft SQL Server databases.
- If your network is geographically dispersed, you may need to install additional management servers for load balancing and bandwidth distribution purposes.

To help you plan medium to large-scale installations, see:

[Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper](#)

For more information, see:

- [Network architecture considerations](#)
- [Setting up sites and replication](#)
- [Setting up failover and load balancing](#)

Step 2: Prepare for and then install Symantec Endpoint Protection Manager

1. Make sure the computer on which you install the management server meets the minimum system requirements. See: [Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)
2. To install Symantec Endpoint Protection Manager, you must be logged on with an account that grants local administrator access.
3. Decide on whether to use the default Microsoft SQL Server Express database or a Microsoft SQL Server database. If you use a Microsoft SQL Server database, the installation requires additional steps. These include, but are not limited to, configuring or creating a database instance that is configured to use mixed mode or Windows authentication mode. You also need to provide database server administration credentials to create the database and the database user. These are specifically for use with the management server. See:
 - [About SQL Server configuration settings](#)
 - [Setting up failover and load balancing](#)
4. You install Symantec Endpoint Protection Manager first. After you install, you immediately configure the installation with the Management Server Configuration Wizard.
Decide on the following items when you configure the management server:
 - A password for your logon to the management console
 - An email address where you can receive important notifications and reports
 - An encryption password, which may be needed depending on the options that you select during installationFor more information, see:
 - [Installing Symantec Endpoint Protection Manager](#)
 - [About basic management server settings](#)
 - [Configuring Symantec Endpoint Protection Manager after installation](#)

Step 3: Add groups, policies, and locations

1. You use groups to organize the client computers, and apply a different level of security to each group. You can use the default groups, import groups if your network uses Active Directory or an LDAP server, or add new groups.
If you add new groups, you can use the following group structure as a basis:
 - Desktops
 - Laptops
 - ServersFor more information, see:
 - [Importing existing groups and computers from an Active Directory or an LDAP server](#)
 - [How you can structure groups](#)
 - [Adding a group](#)
2. You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall.
A location can allow the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.
For more information, see:
 - [Best Practices for Symantec Endpoint Protection Location Awareness](#)
 - [Adding a location to a group](#)
3. Disable inheritance for the groups or locations for which you want to use different policies or settings.
By default, groups inherit their policies and settings from the default parent group, **My Company**. If you want to assign a different policy to child groups, or want to add a location, you must first disable inheritance. Then you can change the policies for the child groups, or you can add a location.

NOTE

Symantec Endpoint Protection Manager policy inheritance does not apply to the policies that are received from the cloud. The cloud policies follow the inheritance as defined in the cloud.

For more information, see:

[Disabling a group's inheritance](#)

4. For each type of policy, you can accept the default policies, or create and modify new policies to apply to each new group or location. You must add requirements to the default Host Integrity policy for the Host Integrity check to have an effect on the client computer.

Step 4: Change communication settings to increase performance

You can improve network performance by modifying the following client-server communication settings in each group:

- Use pull mode instead of push mode to control when clients use network resources to download policies and content updates.
- Increase the heartbeat interval. For fewer than 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger environments might need a longer heartbeat interval. Symantec recommends that you leave **Let clients upload critical events immediately** checked.
- Increase the download randomization to between one and three times the heartbeat interval.

For more information, see:

- [Randomizing content downloads from the default management server or a Group Update Provider](#)
- [Updating policies and content on the client using push mode or pull mode](#)

Step 5: Activate the product license

Purchase and activate a license within 60 days of product installation. See:

- [Licensing Symantec Endpoint Protection](#)
- [Symantec Endpoint Protection product license terminology](#)
- [Activating or importing your Symantec Endpoint Protection product license](#)

Step 6: Decide on a client deployment method

Determine which client deployment method would work best to install the client software on your computers in your environment. See:

[Choosing a method to install the client using the Client Deployment Wizard](#)

- For Linux clients, you can use either **Save Package** or **Web Link and Email**, but not **Remote Push**.
- For Windows and Mac clients, if you use **Remote Push**, you may need to do the following tasks:
 - Make sure that administrator access to remote client computers is available. Modify any existing firewall settings (including ports and protocols) to allow remote deployment between Symantec Endpoint Protection Manager and the client computers. See:
[Communication ports for Symantec Endpoint Protection](#)
 - You must be logged on with an account that grants local administrator access.
If the client computers are part of an Active Directory domain, you must be logged on to the computer that hosts Symantec Endpoint Protection Manager with an account that grants local administrator access to the client computers. You should have administrator credentials available for each client computer that is not part of an Active Directory domain. See:
[Preparing Windows and Mac computers for remote deployment](#)

For more information, see:

Preparing for client installation

Step 7: Prepare the client for installation

1. Make sure that the computers on which you install the client software meet the minimum system requirements. You should also install the client on the computer that hosts Symantec Endpoint Protection Manager. See:
[See: Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)
2. Manually uninstall any third-party security software programs from Windows computers that the Symantec Endpoint Protection client installer cannot uninstall.
For a list of products that this feature removes, see:
[Third-party security software removal support in Symantec Endpoint Protection](#)
You must uninstall any existing security software from Linux computers or from Mac computers.
Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.
3. As of 14, you can configure the installation package to remove a Windows Symantec Endpoint Protection client that does not uninstall through standard methods. When that process completes, it then installs Symantec Endpoint Protection. See:
[Configuring client packages to uninstall existing security software](#)

Step 8: Deploy and install the client software

1. For Windows clients, do the following tasks:
 - Create a custom client install feature set that determines which components you install on the client computers. You can also use one of the default client install feature sets. See:
[Importing existing groups and computers from an Active Directory or an LDAP server](#)
For client installation packages for workstations, check the email scanner protection option that applies to the mail server in your environment. For example, if you use a Microsoft Exchange mail server, check **Microsoft Outlook Scanner**.
 - Update custom client install settings to determine installation options on the client computer. These options include the target installation folder, the uninstallation of third-party security software, and the restart behavior. You can also use the default client install settings. See:
[Choosing which security features to install on the client](#)
2. With the Client Deployment Wizard, create a client installation package with selections from the available options, and then deploy it to your client computers. You can only deploy to Mac or Windows computers with the Client Deployment Wizard. See:
 - [Installing Symantec Endpoint Protection clients with Web Link and Email](#)
 - [Installing Symantec Endpoint Protection clients with Remote Push](#)
 - [Installing Symantec Endpoint Protection clients with Save Package](#)
 - [Exporting client installation packages](#)

Symantec recommends that you do not perform third-party installations simultaneous to the installation of Symantec Endpoint Protection. The installation of any third-party programs that make network- or system-level changes may cause undesirable results when you install Symantec Endpoint Protection. If possible, restart the client computers before you install Symantec Endpoint Protection.

Step 9: Check that the computers are listed in the groups that you expected and that the clients communicate with the management server

In the management console, on the **Clients > Clients** page:

1. Change the view to **Client status** to make sure that the client computers in each group communicate with the management server.

Look at the information in the following columns:

- The **Name** column displays a green dot for the clients that are connected to the management server. See: [Checking whether the client is connected to the management server and is protected](#)
 - The **Last Time Status Changed** column displays the time that each client last communicated with the management server.
 - The **Restart Required** column displays whether or not the client computers need to be restarted to be protected. See: [Restarting the client computers from the Symantec Endpoint Protection Manager](#)
 - The **Policy Serial Number** column displays the most current policy serial number. The policy might not update for one to two heartbeats. You can manually update the policy on the client if the policy does not update immediately. See:
 - [Using the policy serial number to check client-server communication](#)
 - [Updating client policies](#)
2. Change to the **Protection technology** view and ensure that the status is set to **On** in the columns between and including **AntiVirus Status** and **Tamper Protection Status**. See: [Viewing the protection status of client computers](#)
 3. On the client, check that the client is connected to a server, and check that the policy serial number is the most current one. See: [Checking the connection to the management server on the client computer](#)

More information

- [Checking whether the client is connected to the management server and is protected](#)
- [Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

Quick Start for Symantec Endpoint Protection

This guide helps you download, install, and configure Symantec Endpoint Protection, and is designed for default, first-time managed installations of 500 clients or fewer.

To upgrade, see:

[Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection \(SEP\)](#)

Preinstall: Check system requirements

Before you install Symantec Endpoint Protection Manager or the Symantec Endpoint Protection clients, perform the following steps:

1. [Download SymDiag](#) and run the preinstall check to ensure the computer(s) meet system requirements.
2. Review the [release notes and system requirements for Symantec Endpoint Protection](#).

Step 1: Download the Symantec Endpoint Protection installation file

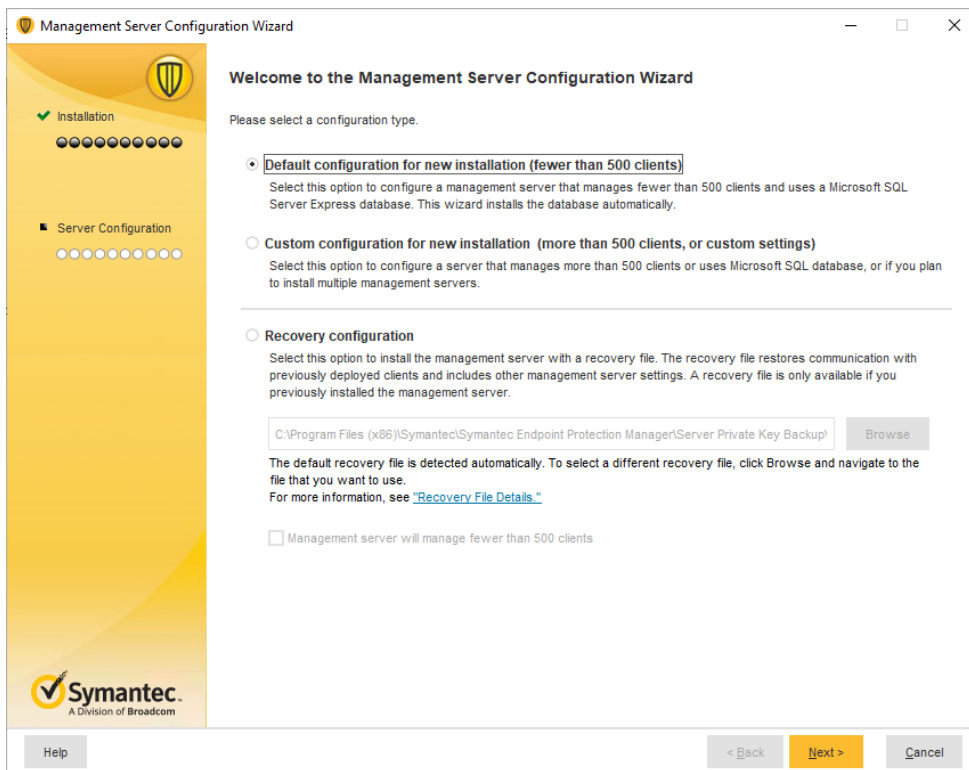
You download the latest version of Symantec software and tools, retrieve license keys, and activate your product through the [Broadcom Support Portal](#). See:

- [Symantec Getting Started](#) and scroll down to **On-Premises Security Products**.
- [Download the latest version of Symantec software](#)

If you cannot find or otherwise download your Symantec software through the Broadcom Support Portal, see [Customer Care](#) or [Sales](#).

Step 2: Install the Symantec Endpoint Protection Manager

1. In the folder where you downloaded the Symantec Endpoint Protection installation file, double-click the file to extract all files. If you see an **Open File - Security Warning** prompt, click **Run**.
The file extracts to C:\Users\username\AppData\Local\Temp\7zXXXXXXXXXX, where XXXXXXXXXX represents a random string of letters and numbers.
 - Setup.exe automatically launches. Leave the installation menu open until the installation completes. Closing the menu deletes all of the files in the temporary directory.
 - To save the installation files, navigate to the previously described temp folder and copy its contents to a location that you select. The installation files include the Tools directory.
2. Click **Install Symantec Endpoint Protection**.
3. Continue with the installation by accepting the terms in the license agreement, along with all default prompts, and then click **Install**.
4. On the **Welcome to the Management Server Configuration Wizard** panel, click **Default configuration**, and then click **Next**.



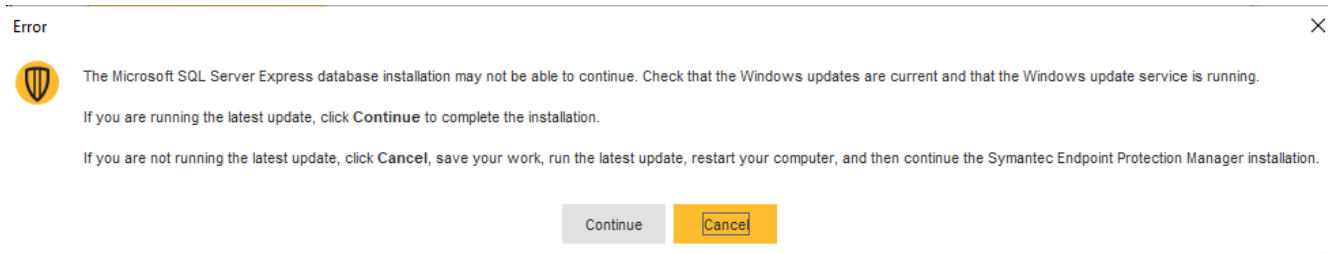
For a customized installation, such as using a SQL Server database, click **Custom configuration**.

See: [Installing Symantec Endpoint Protection Manager with a custom configuration](#)

5. Fill out the required fields to create the system administrator account and email address to which Symantec Endpoint Protection Manager sends notifications, and then click **Next**.
 - Keep `admin` as the user name.
 - You must configure the mail server to receive notification and password reset emails from the management server. You can also enter specified mail server information, and then click **Send Test Email** (optional).
6. Choose the following options, and then click **Next**:
 - Whether or not Symantec collects pseudonymous data from the clients.
 - Partner information, if it applies to your licensing situation.

NOTE

If you see the following message, click **Continue** unless you need to run the Windows updates.



This step may take some time to finish.

7. On the **Configuration completed** panel, click **Finish** to launch Symantec Endpoint Protection Manager.
8. On the Symantec Endpoint Protection Manager logon screen, type the user name and password that you created earlier in step 5 and confirm that you can log on.
Your user name is `admin` by default.

Step 3: Activate your license and add a group

After you log on to Symantec Endpoint Protection Manager, the **Getting Started** screen appears with multiple links to common tasks. For example, you can activate your license or deploy Symantec Endpoint Protection clients.

To open this screen at any time, click **Help > Getting Started Page** in the top right-hand corner of Symantec Endpoint Protection Manager. For video tours of other common tasks within Symantec Endpoint Protection Manager, click **Take a feature tour**.

To activate your product license

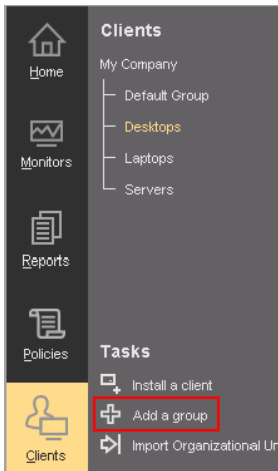
1. In the Symantec Endpoint Protection Manager, in the left pane, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.
3. Using your serial number or the .SLF license file that your order fulfillment email contains, follow the prompts to install your license.

To add a group for clients

Symantec recommends that you create separate groups for desktops, laptops, and servers.

1. In the Symantec Endpoint Protection Manager, in the left pane, click **Clients**.
2. Under **Clients**, click **My Company**.
3. Under **Tasks**, click **Add a group**.
4. In the **Add Group for My Company** dialog box, type the group name and a description, and then click **OK**.

You can then further configure the group settings, such as policy inheritance.



Step 4: Install the Symantec Endpoint Protection clients

Before you install the clients by using Symantec Endpoint Protection Manager, check the following items:

- Make sure that the computers can be accessed through the network.
- Make sure that you have administrator credentials for the computers to which you want to deploy.

For unmanaged client installations, see:

[Installing an unmanaged Windows client](#)

1. In Symantec Endpoint Protection Manager, in the left pane, click **Clients**.
2. Under **Clients**, select the group you created previously.
3. Under **Tasks**, click **Install a client**.
4. In the **Welcome to the Client Deployment Wizard** panel, click **New Package Deployment**, and then click **Next**.
5. In the **Install Packages** drop-down list, select the operating system that matches the operating system of the client computers.
6. Choose the following options depending on the operating system you selected in the previous step.
 - **Windows install package:**
 - In the **Install Feature Sets** drop-down list, keep the default setting of **Full Protection for Clients**.
 - In the **Install Settings** drop-down list, keep the default setting of **Default Standard client installation settings for Windows**.

These default settings require a restart. To change the restart settings, you need to add a custom Install Settings package first. After you add the client package, click **Options** to select the custom package. See:

[Creating custom client installation packages in Symantec Endpoint Protection Manager](#)

NOTE

You may not need to restart the Windows computers except in the following circumstances:

[Restarting the client computers from the Symantec Endpoint Protection Manager](#)

- Choose whether to include virus definitions next to **Content Options**, and then click **Next**.
 - **Mac install package:**

Keep the default setting for **Upgrade settings**, and then click **Next**.
 - **Linux install package:**

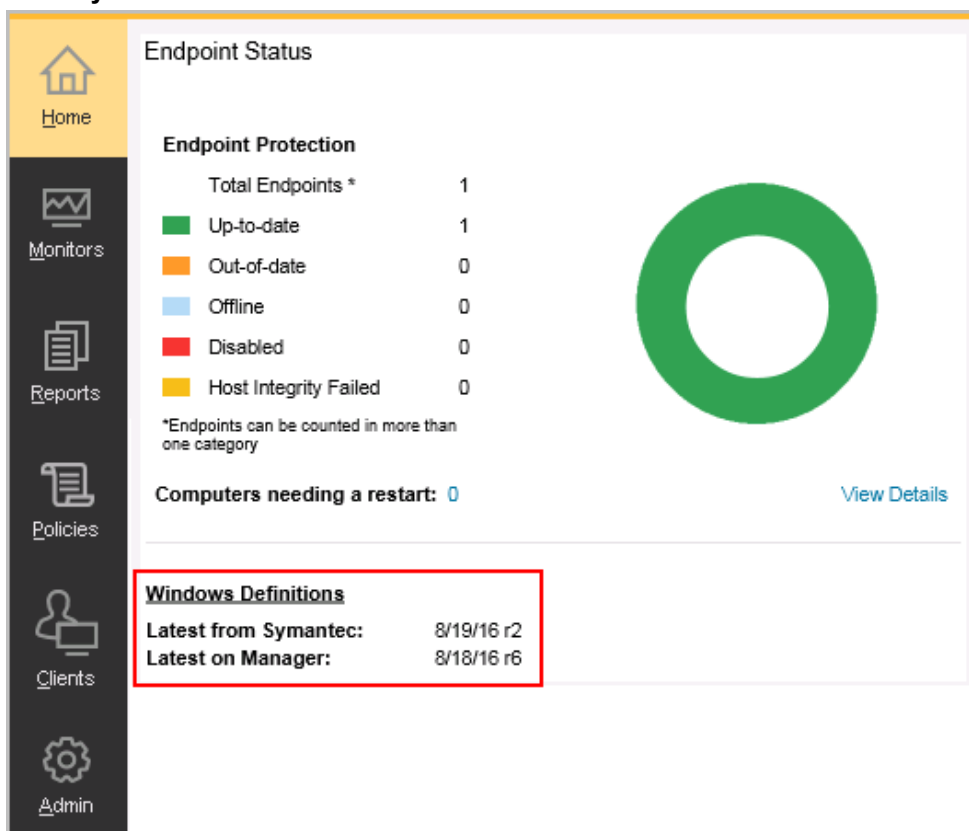
Click **Next**. Linux packages are limited to the **Web Link and Email** or **Save Package** deployment method. See:

 - [Installing the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux](#)
7. Click **Remote Push**, and then click **Next**.

8. On the **Browse Network** tab, browse to your workgroup or domain and select the computers you want to push the Symantec Endpoint Protection client to. After you select the computers, click the >> option to add them to the right pane.
9. After you add the desired computers, click **Next**.
10. Click **Send** to initiate the process.
After the push installation has finished, you see a **Deployment Summary** window with the results of the push.
11. Click **Next**, and then click **Finish** to exit the wizard.
This window indicates that the install files were successfully copied.
12. To confirm that the client was successfully installed, check that the client exists in the client group that you added in the **Clients** pane. See:
[Checking whether the client is connected to the management server and is protected](#)

Step 5: Check that the latest definitions are installed

1. In Symantec Endpoint Protection Manager, in the left pane, click **Home**.
2. In the **Endpoint Status** box, under **Windows Definitions**, compare the dates for **Latest on Manager** and **Latest from Symantec**.

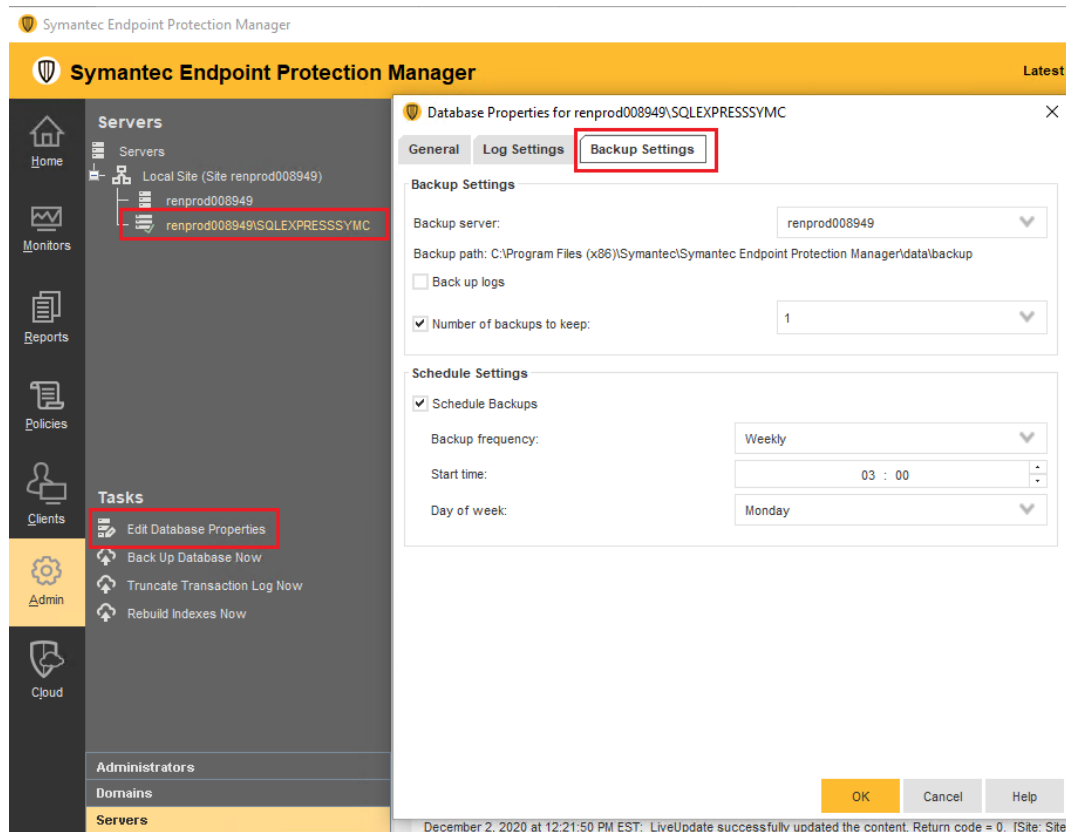


3. If the dates do not match, click **Help** > **Getting Started Page**, click **Run LiveUpdate now**, and then click **Download**.

Step 6: Check the database backup settings

1. In Symantec Endpoint Protection Manager, in the left pane, click **Admin** > **Servers**.
2. Under **Servers**, click **Local Site (My Site)** > **SQLEXPRESSSYMC**.
3. Under **Tasks**, click **Edit Database Properties**.
4. On the **Backup Settings** tab, make any necessary adjustments and then click **OK**.

By default, a backup is saved once a week.



Appendix: Additional resources and guides

- [Product guides and manuals for Symantec Endpoint Protection](#)
- [Best practices for Symantec Endpoint Protection](#)
- [Communication ports that Symantec Endpoint Protection uses](#)
- [External URLs required for Symantec Endpoint Protection \(SEP\) and Symantec Endpoint Security \(SES\)](#)
- [Error: "...services require user rights" or "...cannot read the user rights" during installation or configuration](#)

Managing your clients from the Symantec Endpoint Security cloud

You have the option to manage your devices from both the Symantec Endpoint Protection Manager and the Symantec Endpoint Security cloud. You just enroll the Symantec Endpoint Protection Manager domain into the cloud server any time after installation completes.

See: [Migrating to the SES cloud console](#)

Installing Symantec Endpoint Protection Manager

You perform several tasks to install the management server and the console. In the installation wizard, a green check mark appears next to each completed task.

For the most current system requirements, see:

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

In addition, Symantec Endpoint Protection Manager installation and configuration checks the security policies for the required rights to allow the virtual service accounts to run correctly. Symantec Endpoint Protection Manager automatically

changes local security policies, and alerts you to changes you need to make to domain security policies. You can also change your security policies before installation. See:

[How to assign user rights to the Windows Security Policies for Symantec Endpoint Protection Manager services](#)

NOTE

Symantec Endpoint Protection Manager requires full access to the system registry for installation and normal operation.

NOTE

If you install Symantec Endpoint Protection Manager 14.2 in an IPv6 network, you must also have the IPv4 stack available for Java, even if IPv4 is disabled. If the IPv4 stack is uninstalled, Java does not work, and the Symantec Endpoint Protection Manager installation fails.

To install Symantec Endpoint Protection Manager

1. If you downloaded the product, extract the entire installation file to a physical disk, such as a hard disk. Run **Setup.exe** from the physical disk.

The installation should start automatically. If it does not start, open the installation file, and then double-click **Setup.exe**.

2. In the **Symantec Endpoint Protection Installation Program** dialog box, click **Install Symantec Endpoint Protection**, and then click **Install Symantec Endpoint Protection Manager**.
3. Review the sequence of installation events, and then click **Next** to begin.
4. In the **License Agreement** panel, click **I accept the terms in the license agreement**, and then click **Next**.
5. In the **Destination Folder** panel, accept the default destination folder or specify another destination folder, and then click **Next**.
6. Click **Install**.

The installation process begins for the Symantec Endpoint Protection Manager management server and console. When the installation is complete, click **Next**.

7. After the initial installation completes, you configure the server and database. Click **Next**.
If the management server runs Windows Server 2008 R2, you may see a message to reenab TLS 1.1. You must reenab TLS before you go to the next step. See: [Enabling TLS 1.0 and 1.1 on Microsoft Windows Server 2008 R2 during an installation or upgrade](#)

The **Management Server Configuration Wizard** starts. See:

- [Configuring Symantec Endpoint Protection Manager after installation](#)
- [Installing Symantec Endpoint Protection Manager with a custom configuration](#)

More information

[Getting up and running on Symantec Endpoint Protection Manager for the first time](#)

Configuring Symantec Endpoint Protection Manager after installation

The Management Server Configuration Wizard automatically starts after the Symantec Endpoint Protection Manager installation. You configure the management server according to your requirements.

You can also start the Management Server Configuration Wizard at any time after installation from **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools**. See:

[Installing Symantec Endpoint Protection Manager](#)

To configure Symantec Endpoint Protection Manager after installation

1. With the **Default configuration for new installation** selected, click **Next**.
The default configuration automatically installs the default database, Microsoft SQL Server Express (as of 14.3 RU1). Version 14.3 MPx and earlier installs the embedded database as the default database.
2. Enter company name, a password for the default administrator `admin`, and an email address.
Alternately, you can add details to use a specified mail server.
3. Optionally click **Send Test Email**.
Symantec Endpoint Protection Manager sends password recovery information and other important notifications to this email account, so you should not proceed with configuration if you do not receive the email.
4. Once you verify that you receive the test email, click **Next**.
For 14.3 MPx and earlier, indicate whether you want to run LiveUpdate as part of the installation. Click **Next**. As of 14.3 RU1, LiveUpdate runs automatically as part of a new installation.
5. You can also add the optional **Partner Information**, if a partner manages your Symantec licenses, and then click **Next**.
6. Indicate whether you want Symantec to receive pseudonymous data, and then click **Next** to begin the database creation.
The database creation can take several minutes.
7. When the database creation completes, click **Finish** to complete the Symantec Endpoint Protection Manager configuration.
The Symantec Endpoint Protection Manager console logon screen appears if you leave the option checked to launch Symantec Endpoint Protection Manager. Once you log on, you can begin client deployment. See:

[Logging on to the Symantec Endpoint Protection Manager console](#)

You can find a configuration summary in the following location on the server where Symantec Endpoint Protection Manager is installed:

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

Installing Symantec Endpoint Protection Manager with a custom configuration

When you want to install Symantec Endpoint Protection Manager with a Microsoft SQL Server database or want to install multiple sites, you should choose **Custom configuration** in the **Management Server Configuration Wizard**. When you select this option, additional settings become available.

NOTE

To provide connectivity to the database, you must install SQL Server client tools on the server that runs Symantec Endpoint Protection Manager.

For more information, see:

[About SQL Server configuration settings](#)

To install Symantec Endpoint Protection Manager with a custom configuration

1. See:
[Installing Symantec Endpoint Protection Manager](#)

-
2. In the **Management Server Configuration Wizard**, click **Custom configuration for new installation**, and then click **Next**.

If you have fewer than 500 computers, Symantec recommends that you click **Default configuration for new installation**. See:

[Configuring Symantec Endpoint Protection Manager after installation](#)

3. Click **Install my first site**, and then click **Next**.

The following options are for advanced installations and do not apply to first-time installations of Symantec Endpoint Protection Manager:

- For **Install an additional management server to an existing site**, see:

[Setting up failover and load balancing](#)

- For **Install an additional site**, see:

- [Setting up sites and replication](#)

- [How to install a second site for replication](#)

- [How replication works](#)

4. On this screen, you can customize the following settings, and then click **Next**:

- Site name
- Server name
- Port numbers

You should contact your network administrator before you make changes to the default Symantec Endpoint Protection Manager port configurations.

- The location of the Symantec Endpoint Protection Manager server data folder

If there is not enough available free space on the drive on which Symantec Endpoint Protection Manager is installed, relocate the server data folder to an alternate drive.

5. On the database selection screen, click **Microsoft SQL Server database** and then click **Next**.

- If you select the **Default Microsoft SQL Server Express database** for a custom configuration for 5,000 clients or less, go to step 9. However, the rest of this procedure assumes that you select the Microsoft SQL Server database.
- Check with your SQL database administrator to confirm whether or not the automatic database maintenance tasks should be enabled.
- Symantec recommends that you host the SQL Server and Symantec Endpoint Protection Manager on separate physical servers.
- For information on supported versions of Microsoft SQL Server, see:
[Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security](#)

6. Click **Create a new database**, and then click **Next**.

NOTE

Using an existing database is considered an advanced installation option, and typically does not apply to new installations.

7. On the **Step One: Database Server Authentication** screen, fill in the details for the SQL Server to which Symantec Endpoint Protection Manager connects, and then click **Connect to database**.

If the database connection is successful, the **Step Two: New Database Creation** section becomes available.

8. Under **Step Two: New Database Creation**, fill in the details to create a new database, and then click **Next**.

For questions regarding either **Database Server Authentication** or **Database Creation**, contact your SQL Server database administrator.

If you want to use SQL Server in the FIPS 140-2-compliant mode, you must enable the FIPS before you start SQL Server. If you see the following message and you want to enable FIPS mode, click **Yes** to enable the option to ensure that the management server performs certificate validation.

The screenshot shows the Symantec Endpoint Protection Manager configuration window. On the left is a yellow sidebar with three radio buttons. The main window has two sections. The first section contains four input fields: 'Authentication type' (SQL Server Authentication), 'Database server' (XX.XX.XXX.XX), 'SQL server port' (1433), and 'SQL Server client folder' (C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn) with a 'Browse' button. The second section is titled 'Step Two: Existing Database Parameters' and contains three input fields: 'Database name' (sem5), 'Database user name' (sem5), and 'Database password' (masked with dots). Overlaid on the bottom is a 'Warning' dialog box with a shield icon. It contains text explaining that Symantec Endpoint Protection Manager (SEPM) uses TLS to connect to the SQL Server database, but SQL Server may use a temporary self-signed certificate that SEPM does not trust. It offers two choices: 1. Ensure Windows trusts the certificate by importing it and clicking 'Yes'. 2. Click 'No' to let SEPM use the server IP address or hostname to trust its source. The 'Yes' button is highlighted with a red box.

Authentication type: SQL Server Authentication

Database server: XX.XX.XXX.XX

SQL server port: 1433

SQL Server client folder: C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn Browse

Step Two: Existing Database Parameters

Database name: sem5

Database user name: sem5

Database password:

Warning

Symantec Endpoint Protection Manager (SEPM) uses TLS to connect to the SQL Server database. However, SQL Server may use a temporary self-signed certificate which the SEPM Windows server does not trust; therefore, the SEPM relies on SQL Server IP address or hostname to trust its source other than the certificate. This may expose you to potential SQL Server spoofing.

You can make one of the following choices:

1. You must ensure that Windows trusts this certificate. Therefore, you must provide the certificate on the server computer by importing it into Windows. See [Ensuring that Windows trusts the SQL Server's certificate..](#) Then, click **Yes** to continue the management server configuration.
2. Click **No** to let the Symantec Endpoint Protection Manager use the server IP address or hostname to trust its source rather than the certificate. Only choose this option if both the Symantec Endpoint Protection Manager and SQL Server database are on a secured network.

Yes No

9. Enter company name, a password for the default administrator admin, and an email address.

Alternately, you can add details to use a specified mail server.

10. Click **Send Test Email**. Once you verify that you receive the test email, click **Next**.

Symantec Endpoint Protection Manager sends password recovery information and other important notifications to this email account, so you should not proceed with configuration if you do not receive the email.

-
11. Create an encryption password, or choose to use a random password, and then click **Next**.

This password is used to protect the communication between clients and Symantec Endpoint Protection Manager, and is stored in the Symantec Endpoint Protection Manager recovery file.

12. Indicate whether you want to run LiveUpdate as part of the installation. If you run LiveUpdate as part of a new installation, content is more readily available for the clients you deploy. Click **Next**

You can also add the optional **Partner Information**, if a partner manages your Symantec licenses.

13. Indicate whether you want Symantec to receive pseudonymous data, and then click **Next** to begin the database creation.

14. After the database is created and initialized (which may take several minutes), click **Finish**.

The Symantec Endpoint Protection Manager console logon screen appears if you leave the option checked to launch Symantec Endpoint Protection Manager. Once you log on, you can begin client deployment. See:

[Logging on to the Symantec Endpoint Protection Manager console](#)

You can find a configuration summary in the following location on the server where Symantec Endpoint Protection Manager is installed:

ProgramFiles\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

For more information, see:

[About choosing a database type](#)

Logging on to the Symantec Endpoint Protection Manager console

You log on to the Symantec Endpoint Protection Manager console after you install Symantec Endpoint Protection Manager. You can log on to the console in either of two ways:

1. Locally, from the computer on which you installed the management server.
You can also access the reporting functions from a standalone web browser that is connected to your management server. See:
[Logging on to reporting from a standalone web browser](#)
2. Remotely, from any computer that meets the system requirements for a remote console and has network connectivity to the management server. You can log on to the remote web console or the remote Java console. See:
[Logging on Symantec Endpoint Protection Manager remotely](#)

For security, the console logs you out after a maximum of one hour. You can decrease this period of time. See:

[Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console](#)

Logging on to the Java console (locally)

To log on to the Java console locally

1. Go to **Start > Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**.
2. In the **Symantec Endpoint Protection Manager** logon dialog box, type the user name (`admin` by default) and the password that you configured during the installation.
Optionally check **Remember my user name**, **Remember my password** or both, if available. See:
[Displaying the Forgot your password? link so that administrators can reset lost passwords](#)
 - To log on using a PIV card or CAC, click **Options**, and then check **Log on to a smart card** (14.2 or later). In the **Login / PIN** message, type your pin number. See:

[Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards](#)

- To log on using two-factor authentication, type the password immediately followed by the token. If you omit the token, the logon attempt fails. If you use the Symantec VIP smartphone app, type the password, and then approve the request on the app after you click **Log On**. If you do not approve the request within two minutes, the logon attempt fails. See:

[Configuring two-factor authentication with Symantec VIP](#)

If the console has more than one domain, click **Options** and type the domain name. See: [Adding a domain](#)

3. Click **Log On**.

Logging on to the console remotely

To log on remotely, you need to know the IP address or the host name of the computer on which the management server is installed. Also, make sure that your web browser Internet options let you view content from the server you log on to and that the web browser is supported. For a list of supported web browsers, see:

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

To find the IP address or host name

1. Log on locally.
2. On the **Home** page under **Favorite Reports**, click **Risk Distribution by Protection Technology**.
3. At the bottom of the **Risk Distribution by Protection Technology** dialog box, look for the text: You can launch the Symantec Endpoint Protection Manager using: `http://SEPMServer:9090/symantec.html`.

NOTE

To install the remote console if you haven't already, click `http://SEPMServer:9090/symantec.html` and follow the instructions.

When you log on remotely, you can perform the same tasks as administrators who log on locally. What you can view and do from the console depends on the type of administrator you are. Most administrators in smaller organizations log on as a system administrator. On Microsoft Windows Server 2008 and Windows 7, you must have administrative privileges on the computer where you access the remote console and you must run it using administrative privileges. You can configure the console icon or **Start** menu item to launch using your administrative privileges.

To launch the Java console with administrator privileges

1. Right-click the **Symantec Endpoint Protection Manager Console** icon on the Windows desktop or the **Symantec Endpoint Protection Manager Console** entry on the **Start** menu.
2. Click **Properties > Advanced > Run as Administrator** or **More > Run as administrator**.

For Windows Server 2016, use the host name of the computer on which the management server is installed.

NOTE

If you installed the remote Java console with an earlier version of the product, you must reinstall it when you upgrade to a later version. Starting in 14.3, you cannot log on to the Symantec Endpoint Protection Manager thick remote console if you run a 32-bit version of Windows. The Oracle Java SE Runtime Environment no longer supports 32-bit versions of Microsoft Windows. As of 14.3, the remote web console uses JRE version 11.

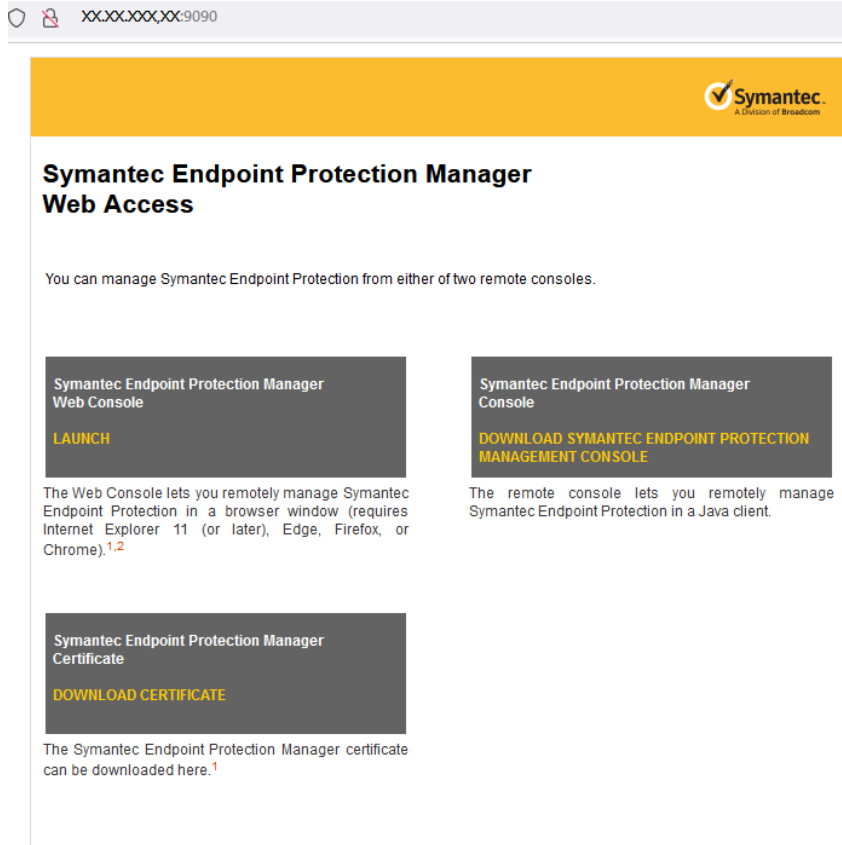
To log on to the web console

1. Open a supported web browser and type the following address in the address box:

`http://SEPMServer:9090/`

Where SEPMServer is the host name or IP address of the management server.

IP addresses include IPv4 and IPv6 (14.2 and later). You must enclose the IPv6 address with square brackets. For example: `http://[SEPMServer]:9090/`



2. On the Symantec Endpoint Protection Manager console Web Access page, click the desired console type.
 - If you click **Symantec Endpoint Protection Manager Web Console**, a secure webpage loads so you log on remotely without the use of the Java Runtime Environment (JRE).
 - If you click **Symantec Endpoint Protection Manager Console**, the computer from which you log on must have the JRE installed to run the Java client. If it does not, you must download and install it. Follow the prompts to install the JRE, and follow any other instructions provided.

The other option is not a remote management solution. You can click **Symantec Endpoint Protection Manager Certificate** to prompt you to download the management console's certificate file. You can then import this file into your web browser if needed.
3. If a host name message appears, click **Yes**.

This message means that the remote console URL that you specified does not match the Symantec Endpoint Protection Manager certificate name. This problem occurs if you log on and specify an IP address rather than the computer name of the management server.

If the webpage security certificate warning appears, click **Continue to this website (not recommended)** and add the self-signed certificate.
4. Follow the prompts to complete the logon process.

When you log on for the first time after installation, use the account name `admin`.

Depending on the logon method, you may need to provide additional information. For instance, if the console has multiple domains, click **Options** and provide the name of the domain to which you want to log on.
5. If you use the Java-based console, you may have the option to save the user name and password. Click **Log On**.

You may receive one or more security warning messages as the remote console starts up. If you do, click **Yes**, **Run**, **Start**, or their equivalent, and continue until the console appears.

You may need to accept the self-signed certificate that the Symantec Endpoint Protection Manager console requires. [Accepting the self-signed server certificate for Symantec Endpoint Protection Manager](#)

More information

[Granting or blocking access to remote Symantec Endpoint Protection Manager consoles](#)

[Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console](#)

Activating or importing your Symantec Endpoint Protection product license

You can use the License Activation Wizard workflow to perform the following tasks:

- Activating a new paid license.
- Converting a trial license to a paid license.
- Renewing a license.
- Activate an additional paid license in response to an over-deployment status.

You can import and activate a license with a file or serial number that you received from your preferred reseller. See:

[Partner Locator](#)

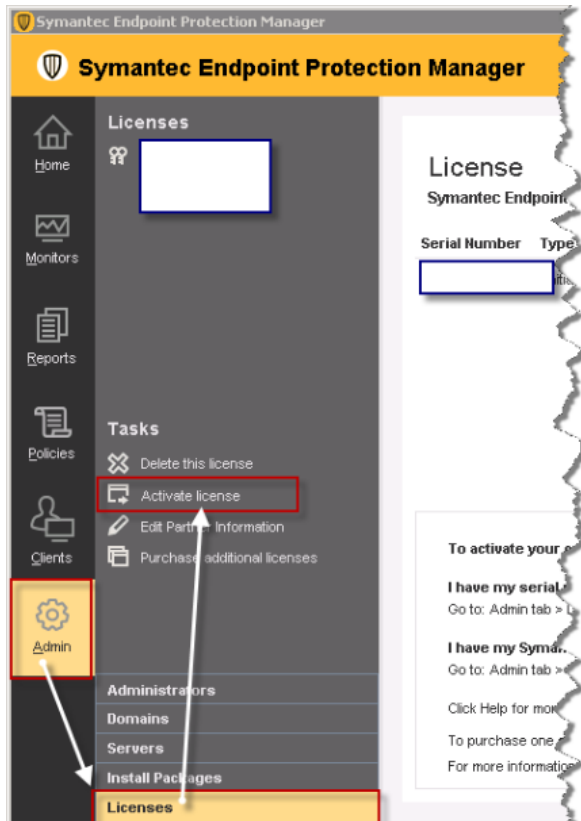
You can start the License Activation Wizard in the following ways:

- The Getting Started screen that appears after you install the product.
You can also access the Getting Started screen through **Help > Getting Started Page**.
- The **Admin** page of the Symantec Endpoint Protection Manager console.

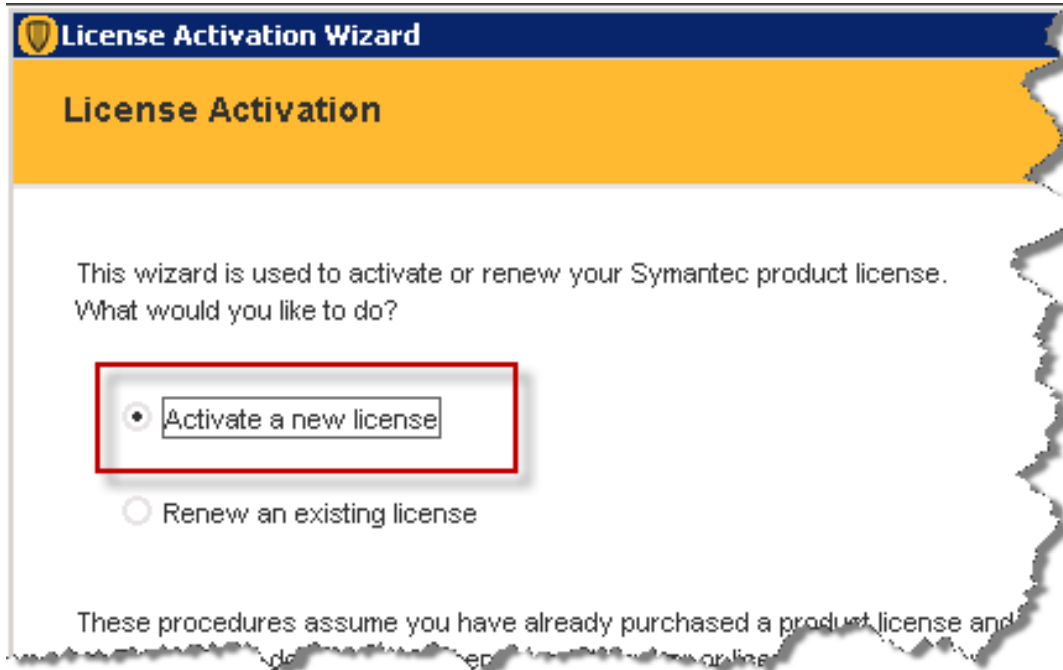
If you activate or import your license from the Getting Started screen, you can skip to step 3.

To activate or import your Symantec Endpoint Protection product license

1. In Symantec Endpoint Protection Manager, click **Admin > Licenses**.
2. Under **Tasks**, click **Activate license**.



3. Click **Activate a new license**, and then click **Next**. If you do not see this panel, continue to the next step.



4. On the **License Activation** panel, select the option that matches your situation, and then click **Next**.

License Activation Wizard

License Activation

License activation requires that you enter a license serial number or select a license serial number or Symantec license file in an email after you purchase your product.

☒ I have a serial number

☐ I have a Symantec License file (.slf) [? What's this?](#)

These procedures assume you have already purchased a product license and a license file is available. If you do not have a license serial number or license file, contact your reseller or partner.

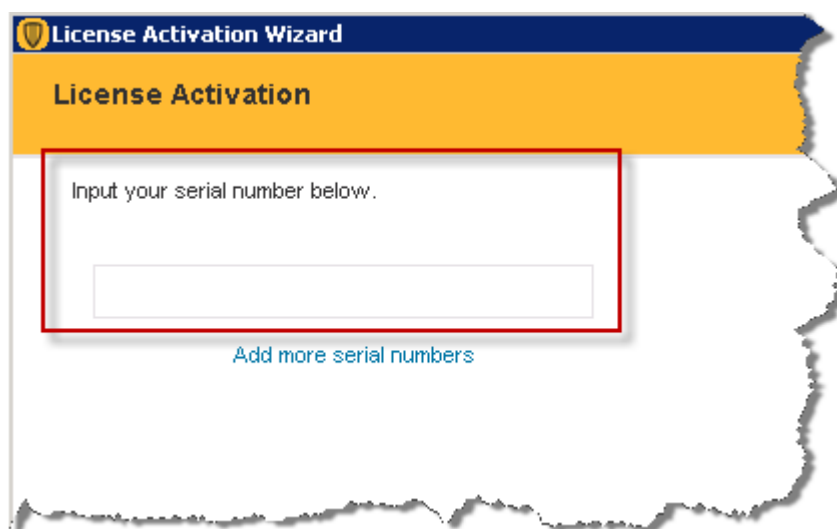
The following table describes each option:

Option	Description
I have a serial number	You may receive a license serial number when you or your preferred reseller purchased the license. If you have a license serial number, select this option. If you have a serial number, select I have a Symantec License File .
I have a Symantec License File (.slf)	In most cases, you receive a Symantec license file (.slf file) in an email from Broadcom shortly after you complete the purchase process. The file arrives attached to the notification email as a .zip file. If you have received a .slf file, select this option. Note: You must extract the .slf file from the .zip file before you can use it to activate your product license. Warning! The .slf file contains the information that is unique to your license. To avoid corrupting the license file, do not alter its contents. You may copy the file for your records.

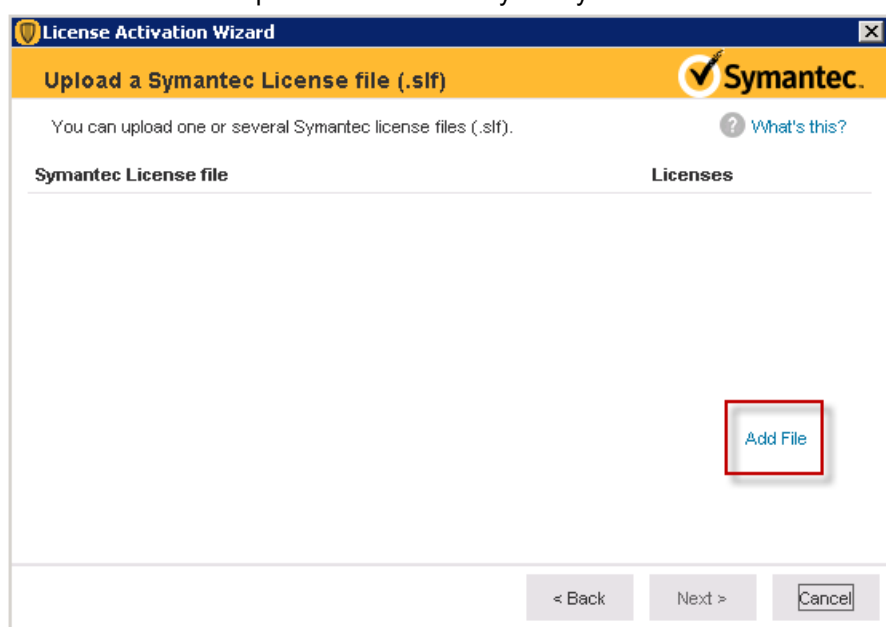
5. Do one of the following tasks based on the selection that you made in the previous step:
 - If you selected **I have a serial number**, enter the serial number, and then click **Submit**. Review the information about the license you added, and then click **Next**.

NOTE

To activate a license with a serial number, you must have an active internet connection and be able to reach the Symantec Licensing Server. If the connection succeeds, the Symantec home page loads.



- If you selected **I have a Symantec License File (.slf)**, click **Add File**. Browse to and select the .slf file you extracted from the .zip file that came with your Symantec notification email. Click **Open**, and then click **Next**.



6. Enter information about your technical contacts and primary contacts, and about your company. Click to acknowledge the disclosure statement, and then click **Submit**.
If you provided this information when you purchased your license, this panel does not display.
7. Click **Finish**.

More information

- [Purchasing Symantec Endpoint Protection licenses](#)
- [Licensing Symantec Endpoint Protection](#)

Purchasing Symantec Endpoint Protection licenses

You need to purchase a license in the following situations:

-
- Your trial license expired. Symantec Endpoint Protection comes with a trial license that lets you install and evaluate the product in your environment.
 - Your current license is expired.
 - Your current license is over-deployed. Over-deployed means that you have deployed more clients than your current license allows.

Depending upon how you purchase your license, you receive by email either a product license serial number or a Symantec License file. The license file uses the file extension .slf. When you receive the license file by email, it is attached to the email as a .zip file. You must extract the .slf file from the .zip file.

To purchase or renew a license

1. Contact your preferred reseller. See:
[Find a Partner or Distributor](#)

Save the license file to a computer that can be accessed from the Symantec Endpoint Protection Manager console. Many users save the license on the computer that hosts Symantec Endpoint Protection Manager. Many users also save a copy of the license to a different computer or removable storage media for safekeeping.

WARNING

To prevent corruption of the license file, do not open or alter the file contents in any way. However, you may copy and store the license as desired.

More information

[Symantec Endpoint Protection product license requirements](#)

[How many Symantec Endpoint Protection licenses do I need?](#)

[Licensing Symantec Endpoint Protection](#)

External URLs required for Symantec Endpoint Protection (SEP)

Symantec Endpoint Protection and the clients communicate with specific URLs to perform multiple functions, such as validating licenses, submitting samples of suspicious files, and communicating with the on-premises Symantec Endpoint Protection Manager or the cloud console. You must allow these URLs if you use one or more proxies in your environment to redirect the necessary traffic to the Symantec servers. See:

[External URLs required for Symantec Endpoint Protection \(SEP\) and Symantec Endpoint Protection \(SES\)](#)

Installing Symantec Endpoint Protection clients with Save Package

If you have a small number of clients, use the Save Package method to deploy and install the installation package on the clients.

Save Package creates the installation packages that you can install manually, with third-party deployment software, or with a login script.

Save Package comprises the following tasks:

- You make your configuration selections and then create the client installation packages.
- You save the installation package to a folder on the computer that runs Symantec Endpoint Protection Manager.
For Windows, the installation package can be for 32- or 64-bit operating systems. The installation package comprises one setup.exe file or a collection of files that includes a setup.exe file. Computer users often find one setup.exe file easier to use.

NOTE

The Mac and Linux client install packages automatically export a .zip archive file format. To correctly preserve the file permissions, you should expand the archive file with a native archive program, such as the Mac Archive Utility or the ditto command. You cannot use the Mac unzip command, a third-party application, or any Windows application to expand the files for these operating systems

To install Symantec Endpoint Protection clients with Save Package

1. In the console, launch the **Client Deployment Wizard**.
2. Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.
3. In the **Client Deployment Wizard**, do one of the following tasks:
 - Click **New Package Deployment**, and then click **Next**. Save Package only installs a new installation package.
 - Click **Communication Update Package Deployment** if you want to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.
4. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

NOTE

To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. See:

[Configuring client packages to uninstall existing security software](#)

For more information, see:

[About the Windows client installation settings](#)

5. Click **Save Package**, and then click **Next**.
6. Click **Browse** and specify the folder to receive the package.

For Communication Update Package Deployment, or for Mac and Linux packages, go to step 7.

For new Windows packages, check **Single .exe file (default)** or **Separate files (required for .MSI)**.

NOTE

Use **Single .exe file** unless you require separate files for a third-party deployment program.

7. Click **Next**.
8. Review the settings summary, click **Next**, and then click **Finish**.
9. Provide the exported package to the computer users.

Provide the exported package to the users in the following ways: email, save the package to a secure shared network location, or use a third-party program.
10. Confirm that the user downloads and installs the client software, and confirm the installation status of the clients.

Mac clients automatically prompt a restart when installation completes. Windows (as of 14.3 RU4) and Linux clients do not require a restart. See:

 - [Running a report on the deployment status of clients](#)

More information

-
- [Restarting the client computers from Symantec Endpoint Protection Manager](#)
 - [Choosing which security features to install on the client](#)
 - [Choosing a method to install the client using the Client Deployment Wizard](#)
 - [Preparing for client installation](#)

Installing Symantec Endpoint Protection clients with Remote Push

Remote Push pushes the client software to the computers that you specify, either by IP address or by computer names. Once the package copies to the target computer, the package installs automatically. The computer user does not need to begin the installation or to have administrator privileges.

Remote Push comprises the following tasks:

- You select an existing client installation package, create a new installation package, or create a package to update communication settings.
- For new installation packages, you configure and create the installation package.
- You specify the computers on your network to receive a package from Symantec Endpoint Protection Manager. Remote Push locates either specific computers for which you provide an IP number or range, or all computers that are visible by browsing the network.

NOTE

To push the client installation package to Mac clients in the **Browse Network** tab, you must install the Bonjour service on the Symantec Endpoint Protection Manager server. See the following article:

[Error deploying the Endpoint Protection client for Mac: "Could not browse the network. The Bonjour service is missing."](#)

[Download Bonjour Print Services for Windows](#)

The Bonjour service does not support IPv6 networking. Macs that only have IPv6 networking enabled cannot display in **Browse Network**.

IPv6 networking is supported as of 14.2.

- Symantec Endpoint Protection Manager pushes the client software to the specified computers. The installation automatically begins on the computers once the package successfully copies to the target computer.

NOTE

You cannot install the Linux client with Remote Push.

To install Symantec Endpoint Protection clients with Remote Push

1. In the console, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

2. In the **Client Deployment Wizard**, do one of the following tasks:

- Click **New Package Deployment** to create a new installation package, and then click **Next**.
- Click **Existing Package Deployment** to use a package that was previously created, and then click **Browse** to locate the package to install.

The Client Deployment Wizard uploads the package and directs you to the **Computer Selection** panel (step 5).
- Under **Communication Update Package Deployment**, choose whether to update Windows or Mac client communication settings on the computers that already have the Symantec Endpoint Protection client installed. Follow the on-screen instructions, and then go to step 4.

Use this option to convert an unmanaged client to a managed client.

For more information, see:

Restoring client-server communications with Communication Update Package Deployment

3. For a new package, in the **Select Group and Install Feature Sets** panel, make selections from the available options, which vary depending on the installation package type. Click **Next**.

NOTE

To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before you launch the Client Deployment Wizard. You can also use an existing client install package that is configured to enable this function. See:

[Configuring client packages to uninstall existing security software](#)

For more information, see:

[About the Windows client installation settings](#)

4. Click **Remote Push**, and then click **Next**.
5. In the **Computer Selection** panel, locate the computers to receive the software using one of the following methods:
 - To browse the network for computers, click **Browse Network**.
 - To find computers by IP address or computer name, click **Search Network**, and then click **Find Computers**.

You can set a timeout value to constrain the amount of time that the server applies to a search.

6. Click > > to add the computers to the list, and authenticate with the domain or workgroup if the wizard prompts you.

The remote push installation requires elevated privileges. If the client computer is part of an Active Directory domain, you should use a domain administrator account.

7. Click **Next**, and then click **Send** to push the client software to the selected computers.

Once the **Deployment Summary** panel indicates a successful deployment, the installation starts automatically on the client computers.

The installation takes several minutes to complete.

8. Click **Next**, and then click **Finish**.
9. Confirm the status of the installed clients on the **Clients** page.

NOTE

After you remotely install the client installation package to Mac clients, you must verify on the client computer that the kernel extension is authorized. Kernel extension authorization is required for Symantec Endpoint Protection to fully function, and Remote Push does not prompt you to authorize if authorization is needed. On the Mac, check the **Security & Privacy** system preference, and click **Allow**.

More information

- [Running a report on the deployment status of clients](#)
- [Restarting the client computers from Symantec Endpoint Protection Manager](#)
- [Preparing for client installation](#)
- [Preparing Windows and Mac computers for remote deployment](#)
- [Choosing which security features to install on the client](#)
- [Choosing a method to install the client using the Client Deployment Wizard](#)

Installing Symantec Endpoint Protection clients with Web Link and Email

The Web Link and Email option creates the installation package and the URL for the installation package. The users receive the URL in an email to download the package and install the Symantec Endpoint Protection client. Users must have administrator privileges to install the package.

Web Link and Email comprises the following tasks:

- You select, configure, and then create the client installation package.
You choose from the options that appear for the configuration of Windows, Mac, and Linux client installation packages. All client installation packages are stored on the computer that runs Symantec Endpoint Protection Manager.
- Email from Symantec Endpoint Protection Manager notifies the computer users that they can download the client installation package.
You provide a list of users to receive an email message, which contains instructions to download and install the client installation package. Users follow the instructions to install the client software.

NOTE

The Mac and the Linux client install packages automatically export a `.zip` archive file format. To correctly preserve the file permissions, you should expand the archive file with a native archive program, such as the `Mac Archive Utility` or the `ditto` command. You cannot use the `Mac unzip` command, a third-party application, or any Windows application to expand the files for these operating systems.

Before you use Web Link and Email, make sure that you correctly configure the connection from the management server to the mail server. See:

[Establishing communication between the management server and email servers](#)

To install Symantec Endpoint Protection clients with Web Link and Email

1. In the console, launch the **Client Deployment Wizard**.
Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.
2. In the **Client Deployment Wizard**, click **New Package Deployment**, and then click **Next**. Web Link and Email only sends a new installation package.
3. Make selections from the available options, which vary depending on the installation package type, and then click **Next**.

NOTE

To uninstall existing security software on the Windows client, you must configure custom Client Install Settings before launching the Client Deployment Wizard. See:

[Configuring client packages to uninstall existing security software](#)

For more information, see:

[About the Windows client installation settings](#)

4. Click **Web Link and Email**, and then click **Next**.
5. In the **Email Recipients and Message** panel, specify the email recipients and the subject.

To specify multiple email recipients, type a comma after each email address. A management console system administrator automatically receives a copy of the message.

You can accept the default email subject and body, or edit the text. You can also copy the URL and post it to a convenient and secure online location, like an intranet page.

-
- To create the package and deliver the link by email, click **Next**, and then click **Finish**.
 - Confirm that the computer users received the email message and installed the client software.
Mac clients automatically prompt a restart when installation completes. Windows (as of 14.3 RU4) and Linux clients do not require a restart. See:

More information

- [Running a report on the deployment status of clients](#)
- [Restarting the client computers from Symantec Endpoint Protection Manager](#)
- [Choosing which security features to install on the client](#)
- [Choosing a method to install the client using the Client Deployment Wizard](#)
- [Preparing for client installation](#)

Installing the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux

The Symantec Endpoint Protection Linux Agent design changed in 14.3 RU1. The graphical user interface was removed, architecture and features changed, and the agent was renamed. This topic mentions features from both agents. You install the Linux Agent and the Symantec Single Agent for Linux the same way. No remote deployment features are available.

14.3 RU1 and later

To install the Linux Agent, create an installation package in Symantec Endpoint Protection Manager, transfer the installation package to a Linux device, and then run the installer. The installer configures the new agent and registers it with Symantec Endpoint Protection Manager.

NOTE

Symantec Linux Agent 14.3 RU1 and later cannot run as an unmanaged device. All management tasks must be performed in Symantec Endpoint Protection Manager or in the cloud console.

Installing the Linux Agent (14.3 RU1 and later)

- In Symantec Endpoint Protection Manager, create and download the installation package.
- Put the package on a network share, USB device, or other share mechanism.
If the devices where you want to install the Linux Agent are in an isolated network or they do not have Internet access, configure a local repository. See:
[Creating a local repository](#)
- Install the Linux Agent in one of the following ways:

If you transferred the package to the Linux device	- Navigate to folder location and run the following command to make the <code>LinuxInstaller</code> file executable: <pre>chmod u+x LinuxInstaller</pre> - Run the following command to install the agent: <pre>./LinuxInstaller</pre>
If you configured a local repository	Run the following command: <pre>./LinuxInstaller -- --local-repo <LOCAL Repository URL></pre> For example: <pre>./LinuxInstaller -- --local-repo https://your-domain.com/sep_linux_agent/14_3RU3</pre>

You must run the command as root.

To view the list of installation options, run `./LinuxInstaller -h`.

-
4. To verify the installation, navigate to `/usr/lib/symantec`. Run `./status.sh` to confirm that the modules are loaded and the daemons are running:

```
./status.sh
Symantec Agent for Linux Version: 14.3.450.1000
Checking Symantec Agent for Linux (SEPM) status..
Daemon status:
cafagent           running
sisamdagent        running
sisidsagent        running
sisipsagent        running
Module status:
sisevt             loaded
sisap              loaded
communication status is only available for cloud-managed clients.
```

14.3 MP1 and earlier

Install a managed or unmanaged Symantec Endpoint Protection client directly to a Linux computer. You cannot deploy the Linux client from Symantec Endpoint Protection Manager remotely. The installation steps are similar whether the client is managed or unmanaged.

The only way to install a managed client is with an installation package that you create in Symantec Endpoint Protection Manager. You can convert an unmanaged client to a managed client by importing client-server communication settings.

If the Linux operating system kernel is incompatible with the pre-compiled Auto-Protect kernel module, the installer tries to compile the kernel module. The auto-compile process automatically launches when needed. If this process fails, Auto-Protect installs but is disabled. For more information, see:

[Supported Linux kernels for Symantec Endpoint Protection](#)

NOTE

You must have superuser privileges to install the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

Installing the Symantec Endpoint Protection client for Linux (14.3 MP1 and earlier)

1. Copy the installation package that you created to the Linux computer. The package is a .zip file.
2. On the Linux computer, open a terminal application window.
3. Navigate to the installation directory with the following command:

```
cd /directory/
```

Where the directory is the name of the directory into which you copied the .zip file.

4. Extract the contents of the .zip file into a directory named `tmp` with the following command:

```
unzip "InstallPackage" -d sepfiles
```

Where `InstallPackage` is the full name of the .zip file, and `sepfiles` represents a destination folder into which the extraction process places the installation files.

If the destination folder does not exist, the extraction process creates it.

5. Navigate to `sepfiles` with the following command:

```
cd sepfiles
```

6. To correctly set the execute file permissions on `install.sh`, use the following command:

```
chmod u+x install.sh
```

-
7. Use the built-in script to install Symantec Endpoint Protection with the following command:

```
sudo ./install.sh -i
```

Enter your password if prompted.

This script initiates the installation of the Symantec Endpoint Protection components. The default installation directory is as follows:

```
/opt/Symantec/symantec_antivirus
```

The default work directory for LiveUpdate is as follows:

```
/opt/Symantec/LiveUpdate/tmp
```

The installation completes when the command prompt returns. You do not have to restart the computer to complete the installation.

For 14.3 MP1 and earlier (graphical user interface)

To verify the client installation, click or right-click the Symantec Endpoint Protection yellow shield and then click **Open Symantec Endpoint Protection**. The location of the yellow shield varies by Linux version. The user interface displays information about program version, virus definitions, server connection status, and management.

More information

- [About auto-compile for the Symantec Endpoint Protection client for Linux](#)
- [About the Linux client graphical user interface](#)
- [Importing client-server communication settings into the Linux client](#)
- [Preparing for client installation](#)

About the Symantec Single Agent for Linux

The Symantec Single Agent for Linux lets you use one agent on your Linux client to communicate with Symantec Endpoint Protection Manager (SEPM) and your Data Center Security (DCS) server.

You don't need to install separate agents on your Linux clients to communicate with SEPM and DCS. The Single Agent for Linux eliminates the need to perform separate agent installations, upgrades, and workflows to manage the agent.

The Single Agent for Linux applies the functionality of the SEP Linux 14.3 RU4 Linux agent and DCS 6.9.2 Linux agent.

The Single Agent for Linux supports the following management options:

- Managed by SEPM and DCS server (dual-managed)

The DCS Manager manages IPS and IDS features. SEPM and the SES cloud manage all other features.

NOTE

In this option, SEPM and SES manages antivirus detection. Antimalware policy configuration from the DCS server is discarded.

SEPM and SES manage all other options (such as Proxy settings, LiveUpdate server, LiveUpdate frequency) in dual-managed mode.

- Managed by SEPM or SES

Only features from SEPM and SES are available. The Single Agent for Linux does not communicate with DCS.

- Managed by DCS manager

Only DCS features are available. The Single Agent for Linux does not communicate with SEPM or SES. CAF services must be disabled, at a minimum.

SEP Linux Agent and DCS Agent upgrade paths to Symantec Single Agent for Linux

Learn the installation sequence to use when you upgrade your SEP Linux Agent and DCS Agent to the Single Agent for Linux.

Previously Installed Agent	Sequence of Installation	Expectation
DCS <= 6.9.1 Installed	Run SEP Installer (>= 14.3.RU4)	Installation/upgrade is not supported and is blocked
	Then Run DCS Installer (>= 6.9.2)	DCS agent upgraded to DCS Mode
DCS <= 6.9.1 Installed	Run DCS Installer (>= 6.9.2)	DCS agent upgraded to DCS Mode
	Then run SEP Installer (>= 14.3.RU4)	Agent configured to Dual Mode
DCS >= 6.9.2 Installed	Run SEP Installer (>= 14.3.RU4)	DCS agent upgraded and configured to Dual Mode
	Then run DCS Installer (>= 6.9.2)	Agent continues to work in Dual Mode
DCS >= 6.9.2 Installed	Run DCS Installer (>= 6.9.2)	DCS agent upgraded to DCS Mode
	Then run SEP Installer (>= 14.3.RU4)	DCS agent configured to Dual Mode
SEP Linux 14.3 RU1/RU2 installed	Run DCS Installer (= 6.9.1)	Installation/upgrade is not supported and is blocked
SEP Linux 14.3 RU1/RU2 installed	Run SEP Installer (>= 14.3.RU4)	Agent upgraded to SEP Mode
	Then run DCS Installer (>= 6.9.2)	Agent configured to Dual Mode
SEP Linux 14.3 RU1/RU2 installed	Run DCS Installer (>= 6.9.2)	Installation/upgrade is not supported and is blocked
	Then run SEP Installer (>= 14.3.RU4)	Agent upgrade to SEP Linux
SEP Linux >= 14.3 RU3 installed	Run DCS Installer (= 6.9.1)	Installation/upgrade is not supported and is blocked
SEP Linux >= 14.3 RU3 installed	Run Linux Installer (>= 6.9.2)	Agent upgraded to SEP Mode
	Then run SEP Installer (>= 14.3.RU4)	Agent configured to Dual Mode
SEP Linux >= 14.3 RU3 installed	Run DCS Installer (>= 6.9.2)	Agent configured to Dual Mode
	Then run SEP Installer (>= 14.3.RU4)	Agent continues to work in dual mode

Getting started on the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux

Get started installing and setting up the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.

NOTE

Both the Symantec Single Agent for Linux and the Symantec Endpoint Protection Linux Agent are referred to in this topic as the Linux Agent.

The Symantec Endpoint Protection Manager administrator may have enabled you to configure the settings on the Linux agent.

Table 15: Steps to get started on the Linux agent (for 14.3 RU1 and later)

Step	Task	Description
Step 1	Install the Linux Agent.	The administrator provides you with the installation package for a managed client or sends you a link by email to download it. See: Installing the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux
Step 2	Check that the Linux agent communicates with the Symantec Endpoint Protection Manager or cloud console.	To confirm the connection to Symantec Endpoint Protection Manager or cloud console, you can run the following command: <code>/usr/lib/symantec/status.sh</code>
Step 3	Verify that the Auto-Protect is running.	To check the status of Auto-Protect, run the following command: <code>cat /proc/sisap/status</code>
Step 4	Check that the definitions are up to date.	LiveUpdate definitions are available at the following location: <code>/opt/Symantec/sdcssagent/AMD/sef/definitions/</code>

Table 16: Steps to get started on the Linux client (for 14.3 MP1 and earlier)

Step	Task	Description
Step 1	Install the Linux client.	The Symantec Endpoint Protection Manager administrator provides you with the installation package for a managed client or sends you a link by email to download it. You can also uninstall an unmanaged client, which does not communicate with Symantec Endpoint Protection Manager in any way. The primary computer user must administer the client computer, update the software, and update the definitions. You can convert an unmanaged client to a managed client. See: Installing the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux
Step 2	Check that the Linux client communicates with Symantec Endpoint Protection Manager.	Double-click the Symantec Endpoint Protection shield. If the client successfully communicates with Symantec Endpoint Protection Manager, then server information displays under Management , next to Server . If you see Offline , then contact the Symantec Endpoint Protection Manager administrator. If you see Self-managed , then the client is unmanaged. The shield icon also indicates both the management and the communication status.
Step 3	Verify that Auto-Protect is running.	Double-click the Symantec Endpoint Protection shield. The Auto-Protect status appears under Status , next to Auto-Protect . You can also check the status of Auto-Protect through the command-line interface: <code>sav info -a</code>
Step 4	Check that the definitions are up to date.	LiveUpdate automatically launches after installation is complete. You can verify that definitions are updated when you double-click the Symantec Endpoint Protection shield. The date of the definitions displays under Definitions . By default, LiveUpdate for the Linux client runs every four hours. If the definitions appear outdated, you can click LiveUpdate to run LiveUpdate manually. You can also use the command-line interface to run LiveUpdate: <code>sav liveupdate -u</code>
Step 5	Run a scan.	By default, the managed Linux client scans all files and folders daily at 12:30 A.M. However, you can launch a manual scan using the command-line interface: <code>sav manualscan -s pathname</code> Note: The command to launch a manual scan requires superuser privileges.

More information

Symantec Single Agent for Linux use cases

The following tables list the actions that occur when upgrading to the Single Agent for Linux:

Symantec Endpoint Protection

Admin	Release	Product Combination	Action
SEP Admin	14.3 RU4	<= 14.3 (AV)	Upgrades AV to 14.3 RU3
		14.3 RU1,2 (AV)	Upgrades AV to 14.3 RU3
		<=6.9.1 (IPS, FIM)	Block if DCS <= 6.9.1
		<=14.3 (AV) AND <= 6.9.1 (IPS/FIM)	Block if DCS <= 6.9.1
		6.9/6.9.1 (AV, IPS, FIM)	Block if DCS <= 6.9.1

DCS

Admin	Release	Product Combination	Action
DCS Admin	6.9.2	<= 14.3 (AV)	N/A
		14.3 RU1,2 (AV)	N/A
		<=6.9.1 (IPS, FIM)	Agent with IPS, FIM, and AMD gets upgraded to 6.9.2

About auto-compile for the Symantec Endpoint Protection client for Linux

For 14.3 MP1 and earlier

The Symantec Endpoint Protection installer for Linux auto-compiles the Auto-Protect kernel module when the operating system kernel is incompatible with the pre-compiled Auto-Protect kernel modules.

Near the end of the installation process, if the client installer detects no active Auto-Protect modules, it launches the auto-compiler to compile the compatible modules.

Previously, Auto-Protect only functioned when the Linux computer's operating system ran a supported kernel. Alternately, you can manually compile the Auto-Protect kernel module.

Prerequisites

Development tools must be present on the Linux client computer for auto-compile to function, such as:

- kernel-devel
- kernel-source
- linux-headers
- build-essentials
- "Development Tools"

Symantec Endpoint Protection kernel modules may not successfully compile on those Linux kernels whose source has been changed. Such Linux kernels are not supported through this feature.

Using auto-compile

Auto-compile automatically launches during installation if needed. You do not need to take any action to launch auto-compile.

If the auto-compile process successfully completes, the terminal window displays the following:

Build Auto-Protect kernel modules from source code successfully

Custom drivers for symap and symev that the auto-compile process creates include **custom** in the file name. The file `sepf1-install.log` also confirms that auto-compile has run and succeeded. By default, this file is saved to `~/`.

If the auto-compile process fails, Auto-Protect installs but remains disabled. The terminal window displays a message similar to the following:

Build Auto-Protect kernel modules from source code failed with error: Number

Number represents the number of the error code, which varies. Refer to your compiler's documentation for information on any error code you receive.

Installing the Symantec Endpoint Protection client for Mac

You can directly install a Symantec Endpoint Protection client on a Mac computer if you cannot use or do not want to use Remote Push. The steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with a package that Symantec Endpoint Protection Manager creates. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Mac client.

NOTE

To prepare the Symantec Endpoint Protection client for Mac for use with third-party remote deployment software, see:

[Exporting and deploying the Endpoint Protection Macintosh client with remote tools](#)

Table 17: Methods for installing the Mac client

If you downloaded the installation file.	1. Extract the contents to a folder on a Mac computer, and then open the folder. 2. Open <code>SEP_MAC</code>. 3. Copy <code>Symantec Endpoint Protection.dmg</code> to the desktop of the Mac computer. 4. Double-click <code>Symantec Endpoint Protection.dmg</code> to mount the file as a virtual disk. You then install the Symantec Endpoint Protection client for Mac
If you have a client installation package .zip from the Broadcom Support Portal. For more information, see: Broadcom Support Portal	1. Copy the file to the desktop of the Mac computer. The file may be named <code>Symantec Endpoint Protection.zip</code> or <code>Symantec_Endpoint_Protection_version_Mac_Client.zip</code>, where version is the product version. 2. Right-click Open With > Archive Utility to extract the file's contents. 3. Open the resulting folder. You then install the Symantec Endpoint Protection client for Mac.

The resulting virtual disk image or folder contains the application installer and a folder called Additional Resources. Both items must be present in the same location for a successful installation. If you copy the installer to another location, you must also copy Additional Resources.

To install the Symantec Endpoint Protection client for Mac:

1. Double-click `Install Symantec Endpoint Protection`.
2. To begin the installation, click **Install**.
3. To install a helper tool that is needed for installing the Symantec Endpoint Protection client, enter your Mac's administrative username and password, and then click **Install Helper**.
4. After the installation, click **Continue** to finish setting up your Symantec Endpoint Protection client.
5. To set up your Symantec Endpoint Protection client, take the following steps:

Authorize the Symantec Endpoint Protection system extension.	In the Security & Privacy dialog box, on the General tab, at System software from application "Symantec Endpoint Protection" was blocked from loading , click Allow . If needed, click the lock icon to make the changes. You must authorize the system extension for Symantec Endpoint Protection to fully function. See: About authorizing system extensions for Symantec Endpoint Protection for macOS 10.15 or later
Allow full disk access.	In the Security & Privacy dialog box, on the Privacy tab, make sure Symantec System Extension is allowed to access data and administrative settings for all users on your Mac device. If needed, click the lock icon to make the changes.
Allow changes to network profile.	When prompted Symantec Endpoint Protection would like to filter network content , click Allow .

6. Click **Complete**.

About authorizing system extensions for Symantec Endpoint Protection for macOS 10.15 or later

Requiring the authorization of system extensions is a security feature of macOS 10.15. You must authorize the system extension for Symantec Endpoint Protection to fully function.

To authorize the system extension for Symantec Endpoint Protection, during the setup of your Symantec Endpoint Protection client, in the **Security & Privacy** dialog box, on the **General** tab, at **System software from application "Symantec Endpoint Protection" was blocked from loading**, click **Allow**.

For more information, see:

[Installing the Symantec Endpoint Protection client for Mac](#)

Managing kernel extension authorization when deploying the Symantec Endpoint Protection client for Mac

If you mass-deploy the Symantec Endpoint Protection client for Mac, you may need to take additional steps to ensure that the kernel extensions are authorized. This requirement applies as of macOS 10.13 (High Sierra). The operating system dictates that the authorization must be made at the local computer. You cannot authorize the kernel extension through remote access, nor can you save the kernel authorization through a preconfigured disk image.

To ensure that kernel extensions are properly authorized on Macs, do one of the following:

- Instruct the Mac users to approve the required extension. Any user can approve a kernel extension through the Security & Privacy preference pane, even if they do not have administrator privileges. See:

About authorizing kernel extensions for Symantec Endpoint Protection for macOS 10.13 or later

- Enroll your Macs in a mobile device management (MDM) solution. Even if you do not actively manage Macs with this solution, kernel extension authorization reverts to the way it was enforced before macOS 10.13.
- As of macOS 10.13.2, authorize the kernel extensions through mobile device management (MDM) with the use of a team identifier. To authorize the kernel extensions for Symantec Endpoint Protection on macOS, use the team identifier 9PTGMPNXZ2. Consult the documentation for your MDM suite for guidance on how to use this team identifier.

NOTE

Starting from Symantec Endpoint Protection client for Mac 14.3, the team identifier is Y2CCP3S9W7 and the system extension name is `com.broadcom.mes.systemextension`

- If you use **NetBoot**, **NetInstall**, or **NetRestore**, use the following command while preparing disk images for deployment:

```
spctl kext-consent add 9PTGMPNXZ2
```

This command uses the Symantec team identifier to pre-approve Symantec kernel extensions on Mac.

Team identifiers that are set through this command are stored in non-volatile random-access memory (NVRAM), which persists even when the Mac powers off. If you reset the NVRAM, the kernel extensions require reapproval. If the user also approved the kernel extension through the Security & Privacy pane, then reapproval is not needed.

For more information on kernel extension loading, see the following Apple documentation:

[Prepare for changes to kernel extensions in macOS High Sierra](#)

What do I do after I install the management server?

The following table displays the tasks to perform after you install and configure the product to assess whether the client computers have the correct level of protection. Continue to perform these tasks regularly, on a weekly or monthly basis.

Table 18: Tasks to perform after you install

Action	Description
Modify the Virus and Spyware Protection policy	Change the following default scan settings: • If you create a group for servers, change the scheduled scan time to a time when most users are offline. See: Setting up scheduled scans that run on Windows computers • Enable Risk Tracer in Auto-Protect. See: For more information, see the article: What is Risk Tracer? Risk Tracer has the following prerequisites: — Network Threat Protection is enabled. See: Running commands on client computers from the console — Windows File and Printer Sharing is enabled. For more information, see: Customizing Auto-Protect for Windows clients
Modify the Firewall policy for the remote computers group and the servers group	• Increase the security for remote computers by making sure that the following default firewall rules for an off-site location are enabled: — Block Local File Sharing to external computers — Block Remote Administration • Decrease the security for the servers group by making sure that the following firewall rule is enabled: Allow Local File Sharing to local computers. This firewall rule ensures that only local traffic is allowed. For more information, see: • Customizing firewall rules • Managing locations for remote clients

Action	Description
Exclude applications and files from being scanned	You can increase performance by configuring the client not to scan certain folders and files. For example, the client scans the mail server directory every time a scheduled scan runs. You should exclude mail server program files and directories from being scanned. For more information, see the article: About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products You can improve performance by excluding the folders and files that are known to cause problems if they are scanned. For example, Symantec Endpoint Protection should not scan the proprietary Microsoft SQL Server files. You should add an exception that prevents scanning of the folders that contain the SQL Server database files. These exceptions improve performance and avoid corruption or files being locked when SQL Server must use them. For more information, see the knowledge base article: How to exclude MS SQL files and folders using Centralized Exceptions In addition, you should exclude false positives from scans. You can also exclude files by extension for Auto-Protect scans on Windows computers. See: • Creating exceptions for Virus and Spyware scans • Customizing Auto-Protect for Windows clients • Customizing Auto-Protect for Mac clients
Run a quick report and scheduled report after the scheduled scan	Run the quick reports and scheduled reports to see whether the client computers have the correct level of security. See: • About the types of Symantec Endpoint Protection Manager reports • Running and customizing quick reports • How to run scheduled reports
Check to ensure that scheduled scans have been successful and clients operate as expected	Review monitors, logs, and the status of client computers to make sure that you have the correct level of protection for each group. See: Monitoring the Symantec Endpoint Protection clients
Assess your content storage and client communication bandwidth requirements	Symantec Endpoint Protection Manager stores the latest full version plus incremental deltas only. This approach means that clients almost always download deltas, not full packages. Only in the rare case where a client is extremely out of date (more than three months), is a full download of the latest content required. See: How to update content and definitions on the clients If your environment must control network bandwidth precisely, you can also throttle client communication. For more information, see the article: Symantec Endpoint Protection Bandwidth Control for Client Communication For more information about calculating storage and bandwidth needs, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper
Configure notifications for a single risk outbreak and when a new risk is detected	Create a notification for a Single risk event and modify the notification for Risk Outbreak. For these notifications, Symantec recommends that you do the following actions: 1. Change the Risk severity to Category 1 (Very Low and above) to avoid receiving emails about tracking cookies. 2. Keep the Damper setting at Auto. Notifications are critical to maintaining a secure environment and can also save you time. See: • Setting up administrator notifications • Managing notifications

More information

- [Getting up and running on Symantec Endpoint Protection for the first time](#)
- [Symantec Endpoint Protection Recommended Best Practices for Securing an Enterprise Environment](#)

Communication ports for Symantec Endpoint Protection

If the computers that run Symantec Endpoint Protection Manager (SEPM) and the Symantec Endpoint Protection (SEP) client also run third-party firewall software or hardware, you must open certain ports. These ports are for remote deployment and for communication between the management server and clients. See your firewall product documentation for instructions to open ports or allow applications to use ports.

By default, the firewall component of Symantec Endpoint Protection already allows traffic on these ports.

WARNING

In 14.3 RU1 and earlier, the firewall in the Symantec Endpoint Protection client is disabled by default at initial installation until the computer restarts. To ensure firewall protection, leave the Windows firewall enabled on the clients until the software is installed and the client is restarted. The Symantec Endpoint Protection client firewall automatically disables the Windows firewall when the computer restarts.

Table 19: Ports for client and server installation and communication

Port	Protocol	Used for	Listening process	Versions
22	TCP	Push deployment from SEPM to Mac computers - Initiated by SEPM (clientremote.exe) - Not configurable	launchd	All
139, 445 137, 138	TCP UDP	Push deployment from SEPM to Windows computers - Initiated by SEPM (clientremote.exe) - Not configurable Also uses TCP ephemeral ports.	svchost.exe	All
443	TCP	Communication between the SEPM (HTTPS) and the SEP client - Initiated by SEP clients - Configurable Clients also use TCP ephemeral ports.	httpd.exe (Apache)	All
443	TCP	Communication between the SEPM and the cloud server For information on which domains to add to the proxy bypass list for the cloud console, see: Proxy error messages appear in the Endpoint Protection Manager Cloud tab > Troubleshooting	prunsrv.exe	All
443	HTTPS	Communication between the SEP roaming client and the Symantec Endpoint Security cloud server Managed clients that have intermittent communication with SEPM upload their critical events directly to the cloud console. SEPM must be enrolled with the cloud console. See: Monitoring roaming Symantec Endpoint Protection clients from the cloud console	None	14.2 and later
514	UDP	Forwarding data to a Syslog server (Optional) - Outbound traffic from Syslog server to SEPM - Inbound traffic to Syslog server - Configurable Traffic to or from SEPM uses UDP ephemeral ports.	SemSvc.exe	
1100	TCP	Remote object registry Tells AjaxSwing on which port to run RMI Registry. - Initiated by AjaxSwing - Not configurable	SemSvc.exe	All

Port	Protocol	Used for	Listening process	Versions
1433	TCP	Communication between a remote SQL Server database and SEPM - Initiated by SEPM - Configurable EPM also uses TCP ephemeral ports.	sqlserver.exe	All
2638	TCP	Communication between the automatically installed database and SEPM - Initiated by SEPM - Configurable	- sqlserver.exe (SQL Server Express database; 14.3 RU1 and later) - dsrv16.exe (embedded database; 14.3 MP1 and earlier)	All
2967	TCP	Group Update Provider (GUP) web-caching proxy functionality - Initiated by SEP clients - Configurable	ccSvcHst.exe	All
2968	TCP	Web and Cloud Access Protection Client Authentication - Initiated by SEP clients - Configurable	ccSvcHst.exe	14.2 and later
8014	TCP	Communication between SEPM (HTTP) and the SEP client - Initiated by SEP clients - Configurable Clients also use TCP ephemeral ports.	httpd.exe (Apache)	All
8081 8082	HTTP HTTPS	Communication between SEPM and the Content Analysis server appliance or the Malware Analysis Appliance.	SEPM	14.2.x versions only. Deprecated in 14.3.
8443	TCP	Server communication (HTTPS). All logon information and administrative communication takes place using this secure port. - Initiated by the Java-based remote console or web-based remote console, or by replication partners - Configurable SEPM listens on this port.	SemSvc.exe	All
8445	TCP	Used by the remote reporting console. - Initiated by the reporting console - Configurable	httpd.exe (Apache)	All
8446	TCP	Web services Remote management applications use this port to send web services traffic over HTTPS. - Initiated by Remote Monitoring and Management (RMM) and by EDR - Configurable - Used for Java Remote Console	semapisrv.exe	All

Port	Protocol	Used for	Listening process	Versions
8447	TCP	Process launcher This virtual service account launches any SEPM processes that require higher privileges, so that these other services do not need to have them. Only honors requests from localhost. - Initiated by SEPM (SemSvc.exe) - Configurable	semlaunchsrv.exe	All
8765	TCP	Server control Used by SEPM for Tomcat web service for shutdown. - Initiated by SEPM - Configurable	SemSvc.exe	All
9090	TCP	Web console communication This port is used only for initial HTTP communication between the remote management console and SEPM. This initial communication includes installation, and to display the logon screen only. - Initiated by the remote Web console - Configurable Also uses TCP ephemeral ports.	SemSvc.exe	All

- Windows Vista and later contain a firewall that is enabled by default. If the firewall is enabled, you might not be able to install or deploy the client software remotely. If you have problems deploying the client to computers running these operating systems, configure their firewalls to allow the required traffic.
- If you decide to use the Windows firewall after deployment, you must configure it to allow file and printer sharing (port 445).

For more information about configuring Windows firewall settings, see the Windows documentation.

More information

- [About basic management server settings](#)
- [Preparing Windows and Mac computers for remote deployment](#)

Installing and Uninstalling the Management Server and Clients

Plan your installation of Symantec Endpoint Protection Manager and the clients.

Before you install the Symantec Endpoint Protection Manager, you may need to consider the following issues:

- The number of clients in your network.
- Which database you want to use, either the default Microsoft SQL Server Express database or Microsoft SQL Server.
- Whether to set up multiple sites.
- Whether to set up a failover server.

Before you install the Symantec Endpoint Protection clients, you may need to consider the following issues:

- Which features you want to install.
- Which deployment method you want to use.

Network architecture considerations

You can install Symantec Endpoint Protection for testing purposes without considering your company network architecture. You can install Symantec Endpoint Protection Manager with a few clients, and become familiar with the features and functions.

When you are ready to install the production clients, you should plan your deployment based on your organizational structure and computing needs.

You should consider the following elements when you plan your deployment:

- Symantec Endpoint Protection Manager
Administrators use Symantec Endpoint Protection Manager to manage security policies and client computers. You may want to consider the security and availability of the computer on which Symantec Endpoint Protection Manager is installed.
- Remote console
Administrators can use a remote computer that runs the console software to access Symantec Endpoint Protection Manager. Administrators may use a remote computer when they are away from the office. You should ensure that remote computers meet the remote console requirements.
- Local and remote computers
Remote computers may have slower network connections. You may want to use a different installation method than the one you use to install to local computers.
- Portable computers such as notebook computers
Portable computers may not connect to the network on a regular schedule. You may want to make sure that portable computers have a LiveUpdate policy that enables a LiveUpdate schedule. Any portable computers that do not check in regularly do not get other policy updates.
- Computers that are located in secure areas
Computers that are located in secure areas may need different security settings from the computers that are not located in secure areas.

You identify the computers on which you plan to install the client. Symantec recommends that you install the client software on all unprotected computers, including the computer that runs Symantec Endpoint Protection Manager.

More information

[Getting up and running on Symantec Endpoint Protection for the first time](#)

About choosing a database type

Symantec Endpoint Protection Manager uses a database to store information about clients and settings. The database is created as part of the configuration process. You must decide which database to use before you install the management server. You cannot use the console until you have configured the management server to use a database.

Table 20: Databases that Symantec Endpoint Protection Manager uses

Database type	Description
Microsoft SQL Server Express (default; 14.3 RU1 and later) Embedded database (default; 14.3 MP1 and earlier)	The default database is automatically installed with Symantec Endpoint Protection Manager and does not require configuration. The default database supports up to 5,000 clients. You can also install SQL Server Express separately, which does require some configuration. For more information, see: About basic management server settings
Microsoft SQL Server	If you choose to use this option, you must install SQL Server and SQL Server Native Client before you install Symantec Endpoint Protection Manager. For optimal compatibility, you install the version of SQL Server Native Client equal to your version of SQL Server. You should consider purchasing and installing SQL Server for the following reasons: - You must support more than 5,000 clients. Each management server that uses SQL Server can support up to 18,000 clients. If your organization has more clients, you can install another management server. - You want to support failover and load balancing. - You want to set up additional management servers as site partners. See: Determining how many sites you need If you create a SQL Server database, you must first install an instance of SQL Server on either a local or a remote server. You must then configure it for communication with the management server. See: About SQL Server configuration settings

About basic management server settings

The following values represent the default settings when you install the Symantec Endpoint Protection Manager.

You can configure some of the following values only when you install the Symantec Endpoint Protection Manager using a custom configuration.

For more information, see:

- [Installing Symantec Endpoint Protection Manager](#)
- [Communication ports for Symantec Endpoint Protection](#)
- [Account name and password requirements for Symantec Endpoint Protection Manager](#)

Table 21: Basic server settings

Setting	Default	Description
Site Name	My Site (default) Site local host name (custom)	The name of the site as it appears in Symantec Endpoint Protection Manager. Site name is the highest-level container under which all features are configured and run within Symantec Endpoint Protection Manager.
Server name	local host name	The name of the computer that runs Symantec Endpoint Protection Manager.

Setting	Default	Description
Server data folder	SEPM_Install\data	The directory in which the Symantec Endpoint Protection Manager places data files including backups, replicated logs, and other files. The installer creates this directory if it does not exist. The default value for SEPM_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
Encryption password	None	This password encrypts communication between Symantec Endpoint Protection Manager and clients. If you choose the default configuration, the system automatically generates the encryption password for you. From the summary screen, you can print or copy this information to the clipboard. If you choose a custom configuration, you can have the system automatically generate a random password, or you can create your own password. The password can be from 8-32 (14.3 RU5 and later) or 6-32 (14.3 RU4 and earlier) alphanumeric characters. Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed-up database to restore. See: Disaster recovery best practices for Endpoint Protection
User name	admin	The name of the default user that is used to log on to the Symantec Endpoint Protection Manager console for the first time. This value is not configurable.
Password	None	The password that is specified for the admin account during server configuration. You need the original admin password to reconfigure the management server at a later time. Document this password and put it in a secure location.
Email address	None	System notifications are sent to the email address specified.

About SQL Server configuration settings

If you install Symantec Endpoint Protection Manager with a SQL Server database, there are specific configuration requirements for SQL Server.

Before you create the database, Symantec recommends that you install a new instance of SQL Server that conforms to Symantec installation and configuration requirements. You can install a database in an existing instance, but the instance must be configured properly or your database installation fails. For example, if you select a case-sensitive SQL collation, your installation fails.

WARNING

To maximize the security posture of remote SQL Server communications, place both servers in the same secure subnet.

Table 22: Required SQL Server configuration settings

Configuration setting	Installation requirement
Instance name	Do not use the default instance name. Create a name such as SEPM. By default, a database named Sem5 is created in the SQL Server instance when you install Symantec Endpoint Protection Manager. The default name is supported, but can cause confusion if you install multiple instances on one computer.
Authentication configuration	Mixed mode or Windows Authentication mode. See: About SQL Server database authentication modes
sa password	Set this password when you set Mixed Mode authentication.

Configuration setting	Installation requirement
Enabled protocol	TCP/IP
IP addresses for TCP/IP	Enable IP1 and IP2
TCP/IP port numbers for IP1, IP2, and IPALL	Set TCP Dynamic Ports to blank, and specify a TCP port number. The default port is typically 1433. You specify this port number when you create the database. The Symantec Endpoint Protection Manager database does not support dynamic ports.
Remote connections	Must be enabled. TCP/IP protocol must also be specified.

If your database is located on a remote server, you must also install SQL Server client components on the computer that runs Symantec Endpoint Protection Manager. SQL Server client components include `BCP.EXE`. The version number of the SQL Server client components should be the same as the version number of SQL Server that you use. Refer to your SQL Server documentation for installation instructions.

During the Symantec Endpoint Protection Manager database configuration phase of the installation, you select and enter various database values. Understand the decisions you must make to correctly configure the database.

The following table displays the settings that you might need to know before you begin the installation process.

Table 23: SQL Server database settings

Setting	Default	Description
Server name	local host name	Name of the computer that runs Symantec Endpoint Protection Manager.
Server data folder	SEPM_Install\data	Folder in which the Symantec Endpoint Protection Manager places data files including backups, replication, and other Symantec Endpoint Protection Manager files. The installer creates this folder if it does not exist. The default value for SEPM_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.
Encryption password	None	The password that encrypts communication between Symantec Endpoint Protection Manager and clients. The password can be from 8-32 (14.3 RU5 and later) or 6-32 (14.3 RU4 and earlier) alphanumeric characters and is required. Document this password and put it in a secure location. You cannot change or recover the password after you create the database. You must also enter this password for disaster recovery purposes if you do not have a backed-up database to restore. See: Disaster recovery best practices for Endpoint Protection

Setting	Default	Description
Database server	local host name	Name of the computer where SQL Server is installed, and the optional instance name. If the database server was installed with the default instance, which is no name, type either <code>host name</code> or the host's IP address. If the database server was installed with a named instance, type either <code>host name\instance_name</code> or <code>IP address\instance_name</code> . The use of <code>host name</code> only works with properly configured DNS. If you install to a remote database server, you must first install the SQL Server client components on the computer that runs Symantec Endpoint Protection Manager.
SQL Server Port	1433	The port that is used to send and receive traffic to the SQL Server. The use of port 0 is not supported. Port 0 specifies a random, negotiated port.
Database Name	sem5	Name of the database that is created.
Database user name	sem5	Name of the database user account that is created. The user account has a standard role with read and write access. The name can be a combination of alphanumeric values and the special characters ~ # % _ + = : . . The special characters ` ! @ ' \$ ^ & * () - { } [] " \ / < ; > , ? are not allowed. The following names are also not allowed: • sysadmin • server admin • setupadmin • securityadmin • processadmin • dbcreator • diskadmin • bulkadmin
Database password	None	The password that is associated with the database user account. The name can be a combination of alphanumeric values and the special characters ~ # % _ + = : . /. The special characters ! @ * () { } [] ; , ? are not allowed.
SQL Server native client folder	SQL Server 2008: Install directory\100\Tools\Binn SQL Server 2012: Install directory\110\Tools\Binn SQL Server 2014 / 2016 / 2017 / 2019: Install directory\Client SDK\ODBC\110\Tools\Binn	Location of the local SQL native client directory that contains bcp.exe. The installation paths that are shown represent the default paths for Microsoft SQL Server. Install directory represents the installation drive and directory for Microsoft SQL Server. To install the SQL Server native client, see the Microsoft TechNet page appropriate for your version of SQL Server: Installing SQL Server Native Client
Server user name	None	Name of the database server administrator account, which is typically sa.

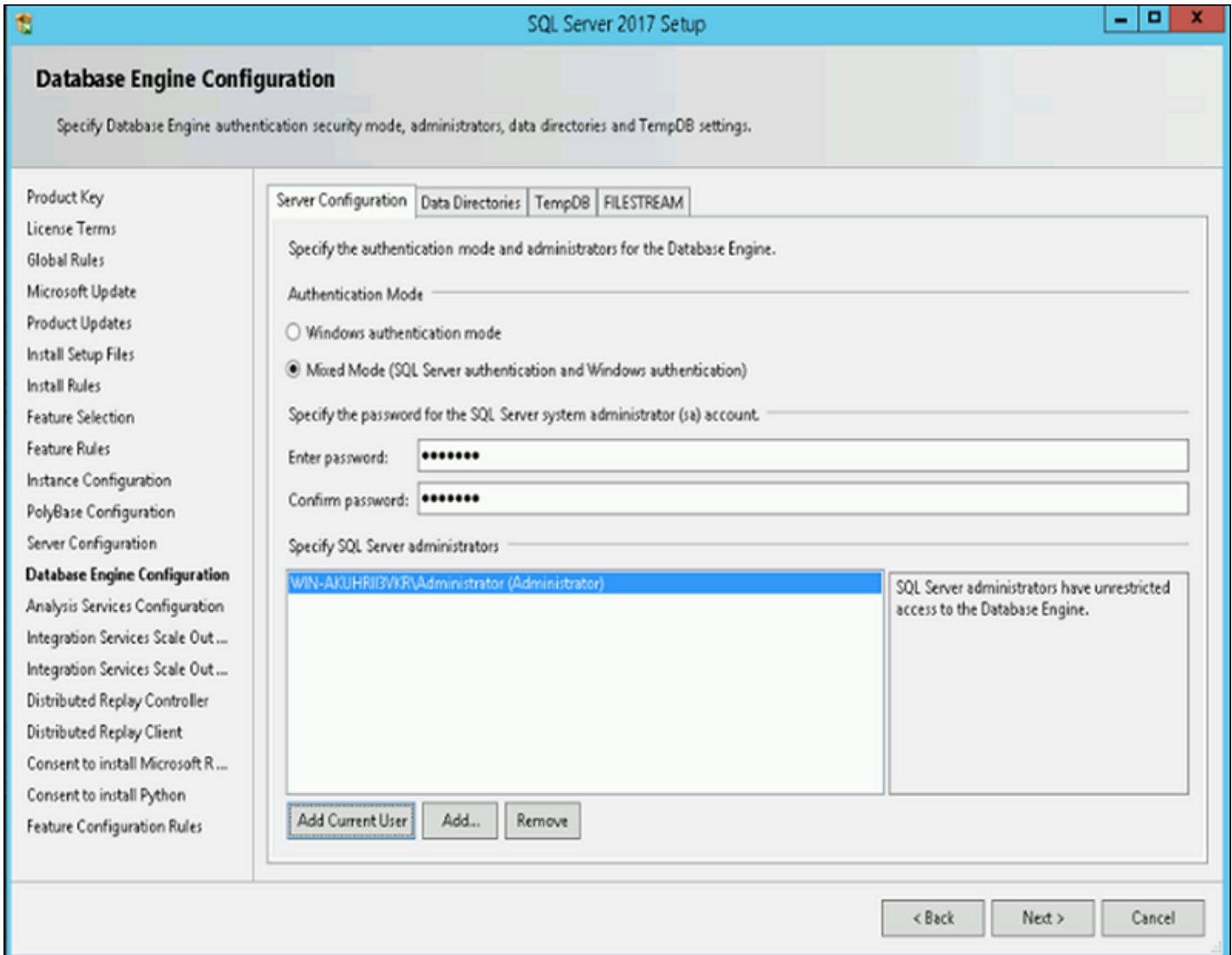
Setting	Default	Description
Server password	None	The password that is associated with the database server administrator account, which is typically sa.
Database data folder	SQL Server 2008: Install directory\MSSQL10.MSSQLSERVER\MSSQL\Data SQL Server 2008 R2: Install directory\MSSQL10_50.MSSQLSERVER\MSSQL\Data SQL Server 2012: Install directory\MSSQL11.MSSQLSERVER\MSSQL\Data SQL Server 2014: Install directory\MSSQL12.MSSQLSERVER\MSSQL\Data SQL Server 2016: Install directory\MSSQL13.MSSQLSERVER\MSSQL\Data SQL Server 2017: Install directory\MSSQL14.MSSQLSERVER\MSSQL\Data SQL Server 2019: Install directory\MSSQL15.MSSQLSERVER\MSSQL\Data	Location of the SQL Server data folder. If you install to a remote server, the volume identifier must match the identifier on the remote server. The installation paths shown represent the default paths for Microsoft SQL Server. • If you install to a named instance on SQL Server 2008, the instance name is appended to MSSQL10. For example, \MSSQL10.instance name\MSSQL\Data • If you install to a named instance on SQL Server 2008 R2, the instance name is appended to MSSQL10_50. For example, \MSSQL10_50.instance name\MSSQL\Data • If you install to a named instance on SQL Server 2012, the instance name is appended to MSSQL11. For example, \MSSQL11.instance name\MSSQL\Data • If you install to a named instance on SQL Server 2014, the instance name is appended to MSSQL12. For example, \MSSQL12.instance name\MSSQL\Data • If you install to a named instance on SQL Server 2016, the instance name is appended to MSSQL13. For example, \MSSQL13.instance name\MSSQL\Data • If you install to a named instance on SQL Server 2017, the instance name is appended to MSSQL14. For example, \MSSQL14.instance name\MSSQL\Data • If you install to a named instance on SQL Server 2019, the instance name is appended to MSSQL15. For example, \MSSQL15.instance name\MSSQL\Data For more information, see: File Locations for Default and Named Instances of SQL Server Note: Clicking Default displays the correct installation folder if you entered the database server and instance name correctly. If you click Default and the correct installation folder does not appear, your database creation fails.

More information

[Installing Symantec Endpoint Protection Manager](#)

About SQL Server database authentication modes

The Symantec Endpoint Protection Manager supports two modes of authentication, based on how you install the SQL Server database.



- **Mixed Mode**

Mixed mode authentication enables both Windows Authentication and SQL Server Authentication. Windows Authentication is always available and can't be disabled. When SQL Server is configured to use mixed mode, you can configure Symantec Endpoint Protection Manager to use either Windows Authentication or SQL Server authentication.

- **Windows Authentication Mode**

Windows Authentication mode enables Windows Authentication and disables SQL Server Authentication. You must configure Symantec Endpoint Protection Manager to use the Windows Authentication mode.

For the remote database connections that use the Windows Authentication mode, be aware of the following requirements:

- For deployments in an Active Directory environment, Symantec Endpoint Protection Manager and SQL Server must be in the same Windows domain.
- For deployments in a Workgroup environment, the Windows account credentials must be the same for the local computers and the remote computers.
- The Windows password must meet the Symantec Endpoint Protection Manager requirements.

- The Windows password must be a maximum of 79 characters and supports the following special characters: `~!@#$%^&*() \ ' ; , . / < > ~ ! @ # $ % ^ & * ( ) \ ' .` If you reconfigure the Symantec Endpoint Protection Manager, the following characters are not allowed: `/ " < > .`
- The following characters were not allowed in earlier versions: `%` and `+` (14.3 RU1 and earlier), `&` (14.3 RU1 and earlier).
- SEPM does not let you paste a Windows password with unallowed characters.

See: [About SQL Server configuration settings](#)

Internationalization requirements

Certain restrictions apply when you install Symantec Endpoint Protection Manager in a non-English or mixed-language environment.

Table 24: Internationalization requirements

Component	Requirements
Computer names, server names, and workgroup names	Non-English characters are supported with the following limitations: • Network audit may not work for a host or user that uses a double-byte character set or a high-ASCII character set. • Double-byte character set names or high-ASCII character set names may not appear properly on the Symantec Endpoint Protection Manager console or on the client user interface. • A long double-byte or high-ASCII character set host name cannot be longer than what NetBIOS allows. If the host name is longer than what NetBIOS allows, the Home, Monitors, and Reports pages do not appear on the Symantec Endpoint Protection Manager console.
English characters	English characters are required in the following situations: • Deploy a client package to a remote computer. • Define the server data folder in the Management Server Configuration Wizard. • Define the installation path for Symantec Endpoint Protection Manager. • Define the credentials when you deploy the client to a remote computer. • Define a group name. You can create a client package for a group name that contains non-English characters. You might not be able to deploy the client package using the Push Deployment Wizard when the group name contains non-English characters, however. • Push non-English characters to the client computers. Some non-English characters that are generated on the server side may not appear properly on the client user interface. For example, a double-byte character set location name does not appear properly on non-double-byte character set named client computers.
User Information client computer dialog box	Do not use double-byte or high-ASCII characters when you provide feedback in the User Information client computer dialog box after you install the exported package. See: Collecting user information
License Activation wizard	Do not use double-byte characters in the following fields: • First name • Last name • Company name • City • State/province

Component	Requirements
Translated languages	In 14.3 RU1 MP1 and earlier, the Symantec Endpoint Protection Manager and the Symantec Endpoint Protection Windows clients were translated from English into the following languages: Chinese, Czech, French, German, Italian, Japanese, Korean, Polish, Brazilian Portuguese, Russian, and Spanish. - In 14.3 RU2, Symantec Endpoint Protection was translated into 4 languages only: French, Japanese, Brazilian Portuguese, and Spanish. - In 14.3 RU4, Symantec Endpoint Protection added support for Simplified and Traditional Chinese. - In 14.3 RU5, Symantec Endpoint Protection added support for Czech, Polish, and Russian. Upgrading Symantec Endpoint Protection Manager 14.3 RU2+ to a supported language

Uninstalling Symantec Endpoint Protection

- [Uninstalling the Windows client](#)
- [Removing specific client components](#)
- [Uninstalling Symantec Endpoint Protect Manager \(SEPM\)](#)
- [What to do when conventional uninstall methods fail](#)
- [Uninstalling the Linux Agent](#)
- [Uninstalling the Mac client](#)

Uninstalling the Windows client

Uninstall a single client or a small group of clients	Use the standard Windows uninstall method
Uninstall a large group of clients, including the remote uninstallation of large groups.	When accessing each client physically is not practical, there are many ways to automate the process. These include: • Uninstalling client software with an Active Directory Group Policy Object • Uninstall the Endpoint Protection client using the command prompt

Remove specific Symantec Endpoint Protection client components

Remove components from a single or unmanaged client	You can remove or add protection components without having to reinstall the client by using Add or Remove Programs or Programs and Features. See: Add or remove features to existing Endpoint Protection clients.
Remove components from a large group of clients	You use the Symantec Endpoint Protection Manager Client Install Feature Set option to modify the installation features on an entire group. See: Add or remove features to existing Endpoint Protection clients.

Uninstall the Symantec Endpoint Protection Manager

The Symantec Endpoint Protection Manager uninstall is fairly straightforward and should be done on a per-management server basis. The following table lists topics that are related to this process.

Perform disaster recovery and back up the Symantec Endpoint Protection Manager	You should back up the Symantec Endpoint Protection Manager first before you uninstall it to make it easier to reconnect with existing clients and use previously configured policies when you reinstall. For information on preparing for disaster recovery, see Disaster recovery best practices for Endpoint Protection Backing up the database and logs
Uninstall the Symantec Endpoint Protection Manager	Use the standard Windows uninstall method . To uninstall Symantec Endpoint Protection Manager, you use the Windows Control Panel for removing, repairing, or changing an application, typically Programs and Features . Uninstalling Symantec Endpoint Protection Manager uninstalls the server and console. You can optionally remove the database and the database backup files during uninstallation.
Reconnect existing clients to a new or reinstalled Symantec Endpoint Protection Manager	If you need to uninstall and reinstall the Symantec Endpoint Protection Manager without performing disaster recovery in advance, then reconnect the existing Symantec Endpoint Protection clients to a new management server installation.

Uninstalling when the conventional methods fail

Sometimes the recommended and preferred methods for uninstalling Symantec Endpoint Protection fail or do not work as expected.	The CleanWipe utility is intended for use only after installing Symantec Endpoint Protection from the Windows Control Panel fails. See: Download the CleanWipe removal tool to uninstall Endpoint Protection .
As a last resort, you can manually remove the Windows client.	See: Manually uninstall Endpoint Protection clients on Windows

Uninstalling the Linux Agent

Run a script to uninstall the agent in groups of any size.	See: Uninstalling the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux
--	---

Uninstalling the Mac client

A single client or small group of clients	See: standard Windows uninstall method
A large group of clients	When accessing each client physically is not practical, there are many ways to automate the process. These include: • Uninstalling client software with an Active Directory Group Policy Object • Uninstall the Endpoint Protection client using the command prompt • Uninstalling the Symantec Endpoint Protection client for Mac
What to do if conventional methods fail	The RemoveSymantecMacFiles utility will remove all files and folders related to the Mac client install. More information and instructions for use can be found in the document Remove Symantec software for Mac OS using RemoveSymantecMacFiles . RemoveSymantecMacFiles/SymantecRemovalTool removes ALL Symantec products from a Mac.

Configuring Symantec Endpoint Protection to be FIPS 140-2-compliant

Set up your network to deploy Symantec Endpoint Protection for FIPS 140-2 compliance.

Federal Information Processing Standards (FIPS) are publicly announced standards that the United States federal government developed to ensure security compliance on computers that are used by non-military government agencies and contractors. FIPS 140-2 standards entail security requirements as they pertain to cryptography modules.

Learn more [about FIPS 140-2-compliance](#) and [which features that FIPS 140-2-compliance does not support](#).

Before you begin

Before you install Symantec Endpoint Protection for the first time, make sure that your version of Symantec Endpoint Protection [supports FIPS compliance](#).

Important notes

- If you upgrade a management server that is already in FIPS mode to a supported Symantec Endpoint Protection version, that management server remains in FIPS mode.
 - If the previous release was not FIPS-compliant, enable FIPS mode.
 - If the previous release used HTTP instead of HTTPS communications, see: [Enabling HTTPS client-server communications](#)
- If you have a site with multiple management servers or multiple sites that replicate with each other, enable FIPS mode on each management server.
- If your site was in FIPS mode and you must recover from a disaster, first [disable FIPS mode](#). After you run the Restore command, reenable FIPS mode.
- After you repair a Symantec Endpoint Protection Manager installation, you must reenable FIPS mode.
- You must disable FIPS mode before you run the Management Server Configuration Wizard. After you run the Wizard, reenable the FIPS mode.
- If you import a new server certificate, you must use a minimum of a 2048-bit key pair. If you do not, you see an `Unexpected server error` message and cannot import the certificate.
- RU7 has more restrictive requirements for the SQL Server database connection. If the upgrade window displays a message that enabling FIPS mode failed, check the `FIPSMODE.log` to fix the issue. Otherwise, the Symantec Endpoint Protection Manager console may not launch.
See: [Troubleshooting FIPS 140-2 compliance issues on Symantec Endpoint Protection](#)

Step 1: Install the Symantec Endpoint Protection Manager (SEPM)

When you install the Symantec Endpoint Protection Manager for the first time, it is not FIPS-compliant by default. Install SEPM before you enable the FIPS mode to avoid certificate problems. The FIPS library deployment script checks that the Symantec Endpoint Protection Manager service is installed before it deploys the FIPS libraries to prevent this issue.

NOTE

FIPS mode only works with a Microsoft SQL Server database and not the default Microsoft SQL Server Express database.

When you configure the Microsoft SQL Server database using the Management Server Configuration Wizard, you may see the following message on the database authentication and creation screen. Select option **1** to perform the certificate validation.

te
adce

Step 4: Enable FIPS compliance on the Microsoft SQL Server

Use the following steps to enforce encrypted communications for all the clients.

- [Enable FIPS mode](#) on the SQL Server computer. Enable the FIPS mode *before* you start SQL Server, because SQL Server reads the FIPS settings at startup.
- Configure the encrypted communications in the SQL Server Configuration Manager:
 - a. In the SQL Server Configuration Manager, expand **SQL Server Network Configuration**, right-click **Protocols for <MSSQLSERVER>**, and then select **Properties**.
 - b. On the **Flags** tab in the **Force Encryption** box, select **Yes**, and then select **OK**.
 - c. Restart the SQL Server service.
- Install the SQL Server certificate.
See: [Installing the SQL Server database certificate](#)

Understanding Symantec Endpoint Protection and FIPS 140-2 level 1 compliance

You deploy Symantec Endpoint Protection in a FIPS 140-2 level 1-compliant configuration to protect client-to-management server, management server-to-management server, and remote administration communication.

The Symantec Endpoint Protection Manager hosts client-to-management-server communications through the Apache web server. For Symantec Endpoint Protection 14.3 or later installations, the Apache server listens on port 443 for encrypted HTTPS connections by default. The HTTPS connection ensures that communications are encrypted and sent through a secure tunnel.

By default, TLS protects client-to-server and client-to-console communication. To protect SQL Server database communications, use encryption.

IMPORTANT

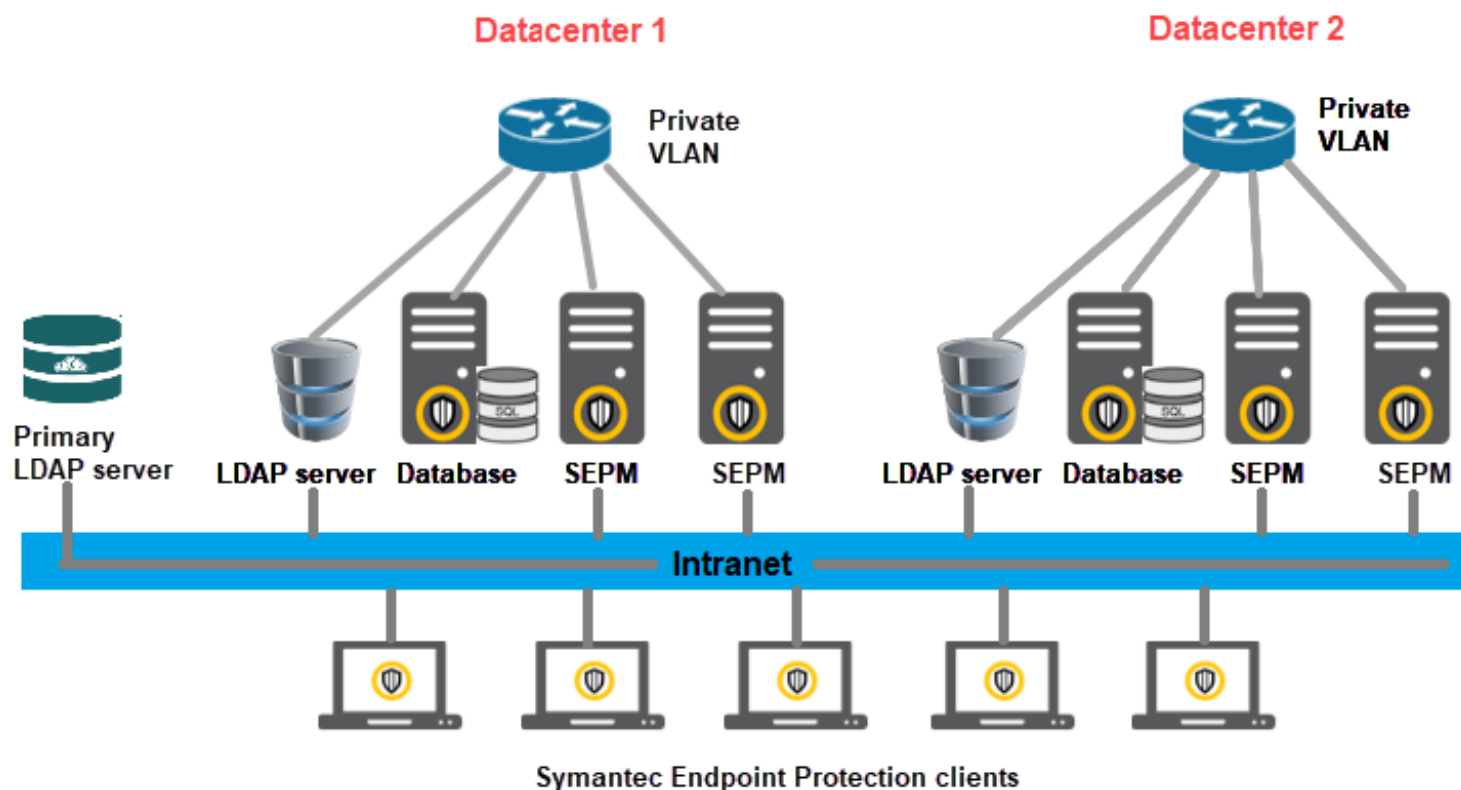
The information that is provided in this document applies to Symantec Endpoint Protection 14.3 RU7 and later Windows clients that use the on-premises deployment. Although you can connect Symantec Endpoint Protection Mac clients and Linux clients to your FIPS-mode server network, these clients do not currently support a FIPS-validated client TLS encryption module.

See: [Unsupported features and limitations in the FIPS 140-2 level 1-compliant mode](#)

Symantec makes the following assumptions about your network environment:

- You use Microsoft domain controllers to provide certificates from a domain controller certificate authority.
- You configured the certificate authority as an enterprise certificate authority that can fulfill certificate requests online to servers that are in the domain.

The following figure illustrates a large-scale deployment with multiple datacenters and Symantec Endpoint Protection Manager sites. A private VLAN network protects database communication within the datacenter. FIPS-validated modules protect the communication to Symantec Endpoint Protection clients and between sites on the intranet.



More information

For information on how to deploy Symantec Endpoint Protection to be FIPS 140-2-compliant	Configuring Symantec Endpoint Protection to be FIPS 140-2-compliant
For information on the versions of Symantec Endpoint Protection that support the FIPS mode	Versions that support FIPS 140-2 level 1 compliance
For a description of FIPS compliance and a list of which cryptographic modules are used in which Windows operating system	FIPS 140 Validation

Versions that support FIPS 140-2 level 1 compliance

Learn which versions of Symantec Endpoint Protection 14.x support FIPS 140-2 level 1 compliance.

Table 25: Symantec Endpoint Protection 14.x and FIPS 140-2 level 1 compliance

14.x versions that support FIPS mode	14.x versions that were not certified for FIPS mode
14.2 and earlier 14.3 RU7 and later	14.3 through 14.3 RU6

The following information applies to installing or upgrading to any supported version of Symantec Endpoint Protection:

- You can upgrade from any unsupported Symantec Endpoint Protection version to a supported Symantec Endpoint Protection version to get FIPS 140-2 level 1 compliance.
- Symantec Endpoint Protection 14.3.x uses a deployment script with libraries that supports FIPS 140-2 level 1 compliance. Apache serves Symantec Endpoint Protection reports on port 8445. If port 8445 is in use, then you should change the reporting website to use a different port during the migration process.

More information

[Enabling or disabling the FIPS mode for the Symantec Endpoint Protection Manager](#)

Unsupported features and limitations in the FIPS 140-2 level 1-compliant mode

Find out which Symantec Endpoint Protection (SEP) features are not supported in FIPS 140-2 level 1-compliant mode.

As of 14.3 RU7, the following features do not work with a Symantec Endpoint Protection deployment that is in FIPS mode:

- Mac and Linux clients. Although you can connect Mac clients and Linux clients to your FIPS-compliant server network, these clients do not currently support a FIPS-validated client TLS encryption module.
- Smart card authentication.
- Syslog communication, which is unencrypted and unsecured.
- Any version of the on-premises Symantec EDR appliance. Symantec plans to support FIPS mode starting with Symantec Endpoint Protection 14.3 RU8 and EDR 4.8.

Some Symantec Endpoint Protection features have not been analyzed or tested for use in a Symantec Endpoint Protection FIPS-compatible deployment. As a best practice, do not use the following Symantec Endpoint Protection features in a FIPS-protected environment:

- Group Update Providers
- Quarantine servers
- Two-factor authentication with Symantec VIP

The FIPS deployment has the following limitations:

- For remote management, Symantec recommends that you use the web console or a connection that uses RDP to access the console locally on the server.
- Because of the increased load that TLS places on performance, Symantec recommends that you have the Symantec Endpoint Protection Manager manage a limited number of clients.

More information

[Configuring Symantec Endpoint Protection to be FIPS 140-2-compliant](#)

Enabling or disabling the FIPS mode for the Symantec Endpoint Protection Manager

Learn how to use a Symantec-supplied script to deploy, enable, disable, and reapply the FIPS-compliant mode for the Symantec Endpoint Protection Manager.

You can double-click the script to check the current FIPS state, on or off. You can also use the `FIPSMODE.vbs` script – `reapply` flag to repair FIPS mode after upgrading or making other changes.

Before you use the enable or disable `FIPSMODE` command, log out of and close the local Symantec Endpoint Protection Manager console, which is Java-based. If you do not log out, some of the files that must be replaced in the enable or disable process are locked, and cannot be replaced. The script prompts you to close any remaining console processes before it can continue.

NOTE

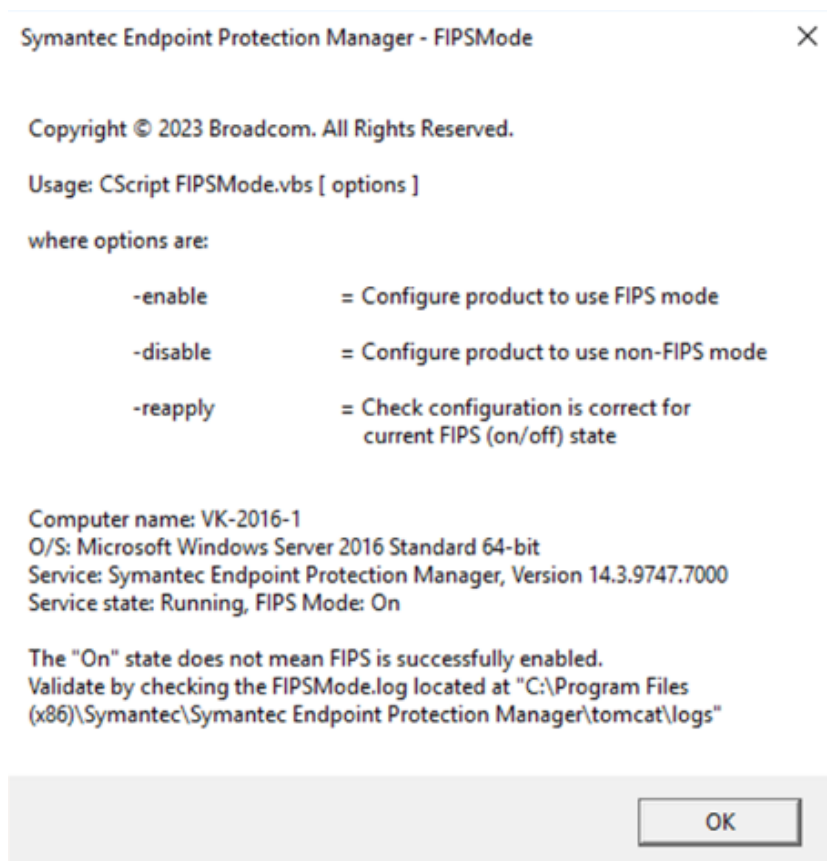
You must disable FIPS mode before you run the Management Server Configuration Wizard, and then reenabling the FIPS mode when you are finished.

NOTE

You can repeat these operations any number of times with no adverse consequences.

To enable the FIPS-compliant libraries

1. Change folder to the C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin folder.
2. Double-click the `FIPSMODE-Enable.bat` file.



To disable the FIPS-compliant libraries

1. Change folder to the C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin folder.
2. Double-click the `FIPSMODE-Disable.bat` file.

To check that FIPS mode is enabled

To verify that the `FIPSMODE-Enable.bat` file enabled FIPS mode successfully, check the log.

1. Go to the C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\logs folder.
2. Open the `FIPSMODE.log`.
3. Look for the entry: `FIPSMODE.vbs has completed successfully.`

More information

- [About the FIPS-compliant libraries](#)
- [Configuring Symantec Endpoint Protection to be FIPS 140-2-compliant](#)

Installing the SQL Server database certificate

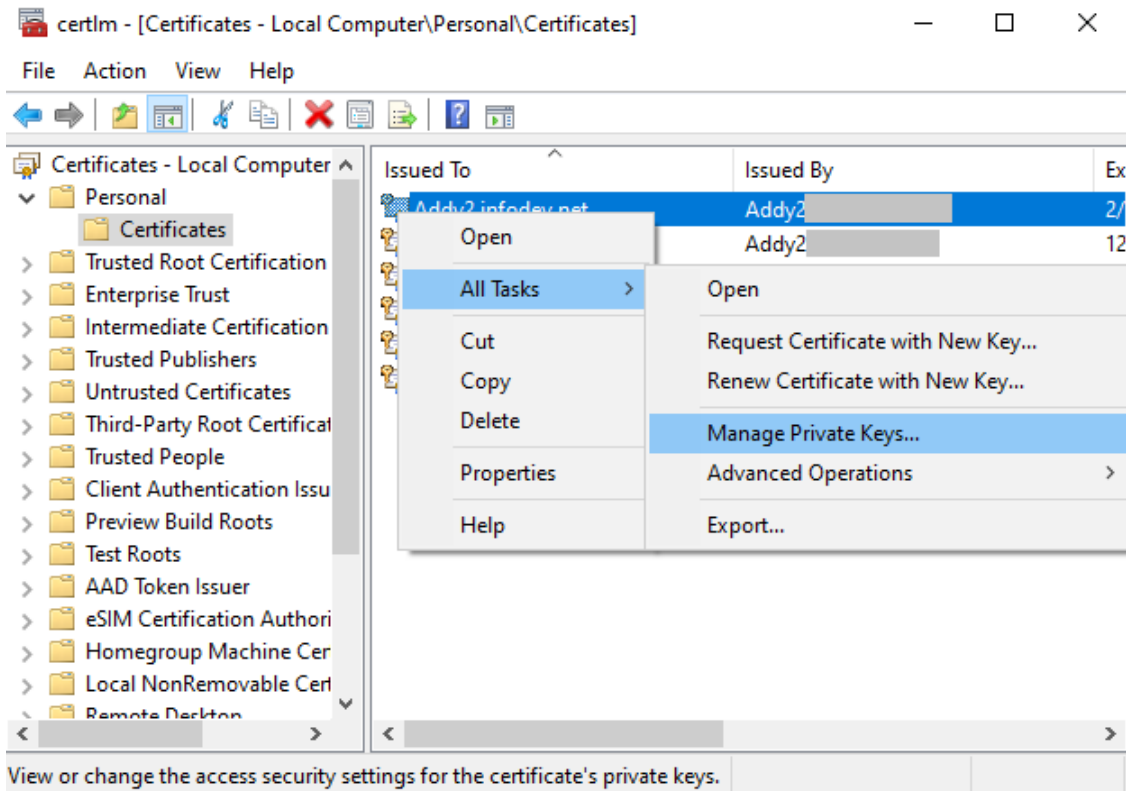
To enforce FIPS 140-2 compliance for Symantec Endpoint Protection clients, you must configure encrypted communications between the SQL Server database and the clients. Follow the steps to install the SQL Server database certificate.

Before you install the SQL Server certificate, make sure that the .pfx or .pem certificate is available on the computer where SQL Server is installed.

Step 1: Check that these certificates are available

Add the Microsoft SQL Server login user to the private key permissions list using the Microsoft Management Console (MMC).

1. Open the Certificate Manager by using the **Run** > `certlm.msc` command.
2. Under **Certificates - Local Computer**, select **Personal** > **Certificates**.
3. In the **Issued To** list, right-click the certificate and click **All Tasks** > **Manage Private Keys**.



4. In the **Permissions for private keys** dialog box, click **Add** to add the SQL Server login user to the permissions list.
5. In the **Enter the object names to select** list, paste the SQL Server login user name.
To get the login user name:
 - a. Go to the Windows **Control Panel** > **Administrative Tools** > **Services** application.
 - b. Double-click the `SQL Server` service.
 - c. On the **Properties** dialog box, click the **Log On** tab, and in the **This account** text field, copy the service name (such as `NT Service\MSSQL$SEM5`).
6. In the **Select Users or Groups** dialog box, paste the service name in the **Enter the object names to select** field.

Select Users or Groups

×

Select this object type:

Users, Groups, or Built-in security principals

Object Types...

From this location:

Locations...

Enter the object names to select [\(examples\)](#):

NT Service\MSSQL\$SEM5

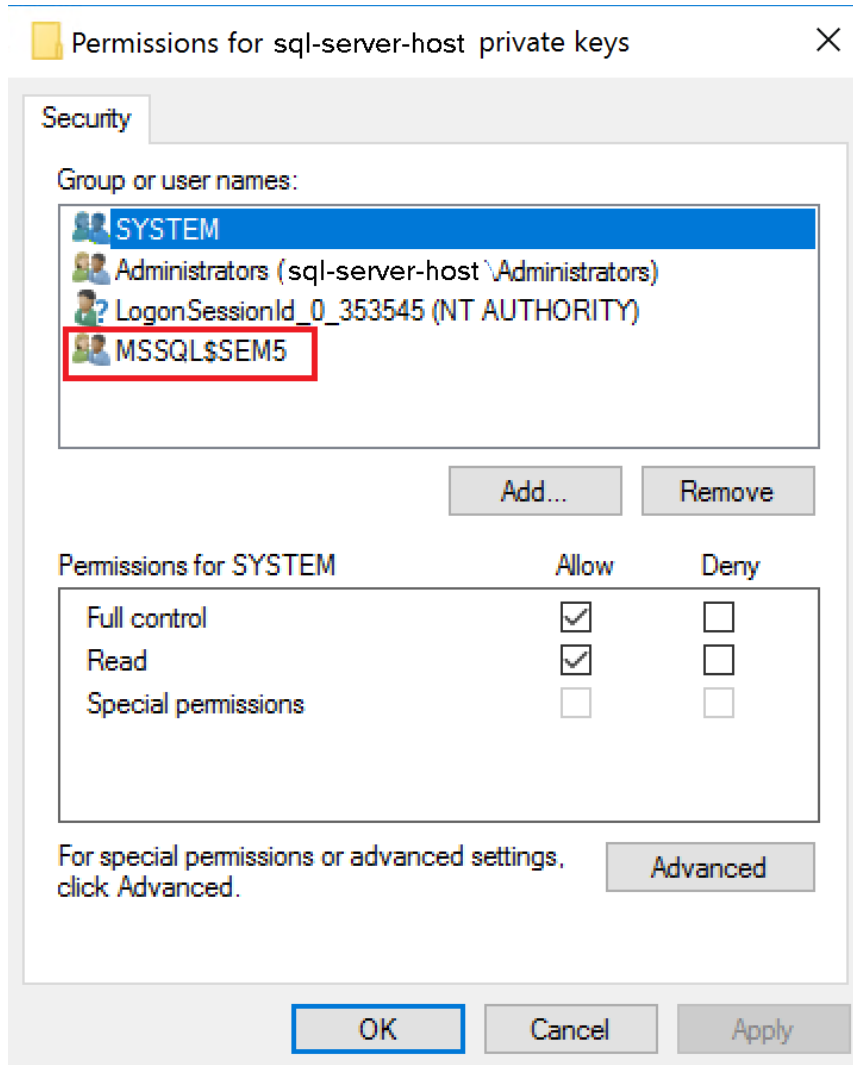
Check Names

Advanced...

OK

Cancel

- You can click **Check Names** to resolve the user name to the full existent name.; though this happens automatically.
7. Click **OK**.



8. Click **OK** > **OK**.

Step 2: Import and install an SSL/TLS certificate (.pfx or .pem) using the SQL Server Configuration Manager

Use the **Subject Alternative Name** field so that any of the following fields match: Host name, DNS name, and IP addresses.

1. In SQL Server Configuration Manager, in the console pane, expand **SQL Server Network Configuration**.
2. Right-click **Protocols for <instance Name>**, and then select **Properties**.
3. On the **Certificate** tab, select the certificate from the **Certificate** drop-down menu, and click **OK**.

Restart the SQL Server service.

More information

[Configuring Symantec Endpoint Protection to be FIPS 140-2-compliant](#)

About the FIPS-compliant libraries

Learn about the Symantec-provided script file that installs the FIPS-compliant libraries.

The script file takes the following actions:

- Stops the Symantec Endpoint Protection Manager service and the Symantec Endpoint Protection Manager webserver service.
- Installs the FIPS-compliant Java and Apache libraries and executables.
- Updates the `java.security` file in the `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\jre\lib\security` folder to install the JCE provider libraries.
- Enables the `FIPSMODE` option in the `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf\ssl\ssl.conf` file.
- Specifies the use of FIPS mode in the `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tomcat\etc\conf.properties` file.
- Adds the following line to configure the pseudo random number generator algorithm to a secure version to the `java.security` file:
`com.rsa.crypto.default.random=HMACDRBG256`
- Installs the OpenSSL FIPS provider (`fips.dll`) and invokes the `openssl fipsinstall` command. This command invokes the required FIPS self-test procedures and creates the `fipsmodule.cnf` configuration file, as required by the OpenSSL FIPS Provider Security Policy document.
- Restarts the Symantec Endpoint Protection Manager service and the Symantec Endpoint Protection Manager webserver service.

As of version 14.3 RU7, SEP uses Bouncy Castle for the Java Secure Socket Extension (JSSE) and crypto providers.

More information

- [Enabling or disabling the FIPS mode for the Symantec Endpoint Protection Manager](#)
- For FIPS certificate and security policy information, see: [Cryptographic Module Validation Program](#)

About the validated modules

Learn which validated modules Symantec Endpoint Protection uses to protect communication.

Table 26: How Symantec Endpoint Protection protects communication: Modules and protected components

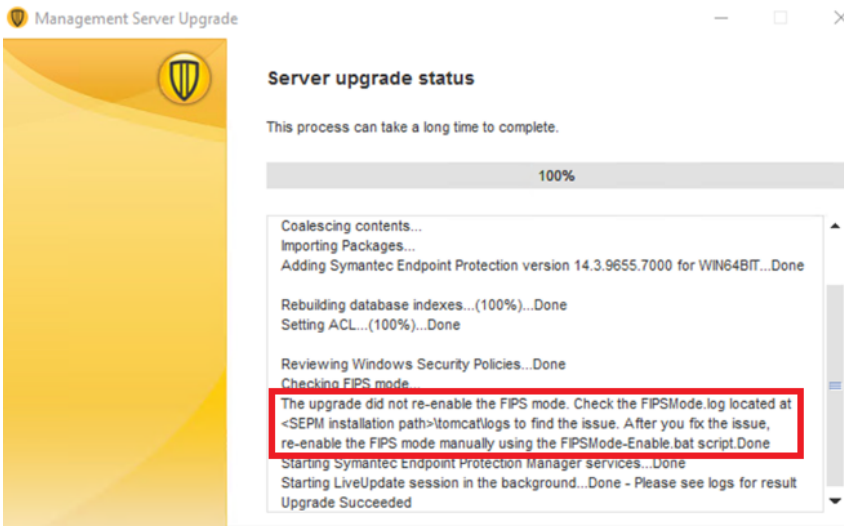
NIST CMVP module certificate number and description	Protected components
Microsoft Windows FIPS Validated Cryptographic Modules: • Cryptographic Primitives Library (<code>bcryptprimitives.dll</code>, <code>ncryptsslp.dll</code>) • Enhanced DSS and Diffie-Hellman Cryptographic Provider (<code>dsenh.dll</code>) (Windows 8 & Server 2012 only) • Enhanced Cryptographic Provider (<code>rsaenh.dll</code>) (Windows 8/Windows Server 2012 only) For information on the latest FIPS validation and certificates for Microsoft Windows modules, see: FIPS 140-2 Validation .	• Symantec Endpoint Protection client TLS connections to Symantec Endpoint Protection Manager (via Windows Schannel) • Windows remote desktop connections • Communications with Microsoft SQL Server
OpenSSL FIPS Provider (OpenSSL 3) See: Cert #4282	Symantec Endpoint Protection Manager Apache server TLS connections
Bouncy Castle FIPS Java API See: Cert #3514	• Symantec Endpoint Protection Manager Tomcat server TLS connections (via Java JCE) • Symantec Endpoint Protection Manager Java console TLS connections (via Java JCE)

More information

[About the FIPS-compliant libraries](#)

Troubleshooting FIPS 140-2 compliance issues on Symantec Endpoint Protection

Table 27: Troubleshooting FIPS 140-2 compliance issues

Issue	Solution
If you upgrade from Windows Server 2019 to Windows Server 2022 and try to log on to a 14.3 RU8 or later SEPM with FIPS enabled, you may see the following error: Unexpected server error. ErrorCode: 0x10010000	Locate the certificate used by the SQL Server that hosts the SEPM database. Import this certificate into the Windows Trusted Root Certificate Authorities. Unable to login to FIPS enabled 14.3 RU8 SEPM after upgrading Operating System
14.3 RU7 has restrictions that earlier SEPM versions didn't have. As a result, you may have issues when you upgrade. If you see the following message, FIPS mode was not enabled successfully. The management console may not launch.	1. Check the <code>FIPSMODE.log</code> to see what the cause of the issue is. Fix the issue. For more information, see "To check that FIPS mode is enabled" at: Enabling or disabling the FIPS mode for the Symantec Endpoint Protection Manager 2. Rerun the <code>FIPSMODE-Enable.bat</code> to reenable FIPS mode. If you don't fix the issue, run <code>FIPSMODE-Disable.bat</code> to ensure that FIPS mode is disabled. SEPM functions normally but not be in FIPS mode.
 Management Server Upgrade Server upgrade status This process can take a long time to complete. 100% - Coalescing contents... - Importing Packages... - Adding Symantec Endpoint Protection version 14.3.9655.7000 for WIN64BIT...Done - Rebuilding database indexes...(100%)...Done - Setting ACL...(100%)...Done - Reviewing Windows Security Policies...Done - Checking FIPS mode - Starting Symantec Endpoint Protection Manager services...Done - Starting LiveUpdate session in the background...Done - Please see logs for result Upgrade Succeeded	After you upgrade the Symantec Endpoint Protection Manager, you may not be sure whether FIPS mode is still enabled.
	Check the <code>FIPSMODE.log</code> file.

[Configuring Symantec Endpoint Protection to be FIPS 140-2-compliant](#)

Managing the Symantec Endpoint Protection client installation

You must install a Symantec Endpoint Protection client on every computer you want to protect, whether the computer is physical or virtual.

Table 28: Client computer installation tasks

Action	Description
Step 1: Identify client computers	Identify the computers on which you want to install the client software. Check that all the computers run a supported operating system. Note: Symantec recommends that you also install the client on the computer that hosts Symantec Endpoint Protection Manager. For the most current system requirements, see: Release notes, new fixes, and system requirements for all versions of Endpoint Protection
Step 2: Identify computer groups (optional)	Identify the computer groups to which you want the clients to belong. For example, you can group clients based on type of computer, to conform to your corporate organization, or to the security level required. You can create these groups before or after you install the client software. You can also import an existing group structure such as an Active Directory structure. See: • Managing groups of clients • Importing existing groups and computers from an Active Directory or an LDAP server
Step 3: Prepare client computers for deployment and installation	If your users do not have administrative rights for their computers, then you should remotely install the client software using Remote Push. The Remote Push installation requires you to enter the credentials that have local administrative rights for the computers. See: Installing Symantec Endpoint Protection clients with Remote Push Prepare the computers for remote client deployment and for successful communication with Symantec Endpoint Protection Manager after installation. See: Preparing Windows and Mac computers for remote deployment
Step 4: Determine features and deploy client software	You deploy the client software using one of the available methods. You can also export a customized client package to deploy later or with a third-party tool. Note: Symantec recommends that you do not perform third-party installations simultaneous to the installation of Symantec Endpoint Protection. The installation of any third-party programs that make network- or system-level changes may cause undesirable results when you install Symantec Endpoint Protection. If possible, restart the client computers before you install Symantec Endpoint Protection. For more information, see: • Choosing a method to install the client using the Client Deployment Wizard • Exporting client installation packages • Installing Windows client software using third-party tools • You decide which features to install to the client computers. You configure custom client feature sets and installation settings before you export or deploy an installation package. Installation settings include the installation folder and the restart settings. You can also use the default client install feature sets and installation settings. See: — Choosing which security features to install on the client — About the Windows client installation settings • For Windows clients, you can choose to automatically uninstall existing third-party security software when you configure client installation settings. See: Configuring client packages to uninstall existing security software
Step 5: Verify installation status	Confirm that the client installation succeeded and that clients communicate with Symantec Endpoint Protection Manager. See: • Symantec Endpoint Protection client status icons

After installation, you can take additional steps to secure unmanaged computers and optimize the performance of your Symantec Endpoint Protection installation.

- [Restarting the client computers from Symantec Endpoint Protection Manager](#)

Preparing Windows and Mac computers for remote deployment

Before you deploy Symantec Endpoint Protection from Symantec Endpoint Protection Manager, you must take steps to prepare the computers to ensure a successful remote installation. These steps pertain only to remote installation. You can reverse these changes afterward, but you must apply them again to perform another remote installation.

NOTE

You cannot deploy the Symantec Endpoint Protection client to Linux computers remotely from Symantec Endpoint Protection Manager.

Table 29: Tasks to prepare all computers for remote deployment

Task	Details
Have administrative rights to your client computers	If the client computer is part of an Active Directory domain, you should use domain administrator account credentials for a remote push installation. Otherwise, have the administrator credentials available for each computer to which you deploy.
Modify firewall settings	Modify firewall settings to allow communication between Symantec Endpoint Protection components. See: Communication ports for Symantec Endpoint Protection
Uninstall existing third-party security software	Uninstall any third-party security software currently in use. For Windows computers, Symantec Endpoint Protection includes a tool to help automatically uninstall select third-party security software. You must separately uninstall any security software that this tool does not uninstall. Note: Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software. You configure this tool before you deploy, and the uninstallation occurs before Symantec Endpoint Protection installs. See: Configuring client packages to uninstall existing security software
Uninstall Symantec Endpoint Protection clients that do not uninstall normally	You can uninstall an existing installation of the Symantec Endpoint Protection client for Windows. You should only use this option if the existing Symantec Endpoint Protection installation does not uninstall normally. You should not use this option as part of a standard deployment. You configure this tool before you deploy, and the uninstallation occurs before Symantec Endpoint Protection installs. See: Configuring client packages to uninstall existing security software
Uninstall unsupported or consumer Symantec security software	Uninstall any unsupported Symantec security software, such as Symantec AntiVirus or Symantec Client Security. Migration directly from these products is not supported. You must also uninstall any consumer-branded Symantec security products, such as Norton Internet Security. See the documentation for your Symantec software for information about uninstallation. For more information, see: Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x

Table 30: Tasks to prepare Windows clients for remote deployment

Operating system	Tasks
Prepare Windows Vista, Windows 7, or Windows Server 2008 / 2008 R2 computers	Windows User Account Control blocks local administrative accounts from remotely accessing remote administrative shares such as C\$ and Admin\$. You do not need to fully disable User Account Control on the client computers during the remote deployment if you disable the registry key LocalAccountTokenFilterPolicy. To disable UAC remote restrictions, see: Description of User Account Control and remote restrictions in Windows Vista Description of User Account Control and remote restrictions in Windows Vista Perform the following tasks: • Disable the Sharing Wizard. The Sharing Wizard prevents more advanced sharing options from working during Remote Push. • Enable network discovery by using the Network and Sharing Center. Network discovery lets you browse the network. You do not need it to search the network. • Enable the built-in administrator account and assign a password to the account. Remote Push fails when the local administrator account has a blank password. If the Windows client computer is part of an Active Directory domain, use domain administrator account credentials with local administrator privileges for Remote Push. • Verify that the account with which you push the installation has administrator privileges. • Enable and start the Remote Registry service. • Disable or remove Windows Defender. Consult the operating system's documentation for guidance on how to successfully complete these tasks.
Prepare Windows 8 / 8.1 or later, or Windows Server 2012 / 2012 R2 or later computers	Before you deploy, perform the following tasks: • Disable the registry key LocalAccountTokenFilterPolicy. To disable UAC remote restrictions, see: Description of User Account Control and remote restrictions in Windows Vista Description of User Account Control and remote restrictions in Windows Vista • Enable and start the Remote Registry service. • Disable or remove Windows Defender.

Table 31: Tasks to prepare Mac clients for remote deployment

Operating system	Tasks
Prepare the Mac computers on any supported operating system	Before you deploy, perform the following tasks on the Mac computers: • Click System Preferences > Sharing > Remote Login and either allow access for all users, or only for specific users, such as Administrators. • If you use the Mac firewall, disable stealth mode. With stealth mode enabled, the remote push installation cannot discover the client through Search Network. To disable stealth mode on the Mac, see the following article and select your version of the Mac operating system. See: Use stealth mode to keep your Mac more secure • Ensure that the firewall does not block the port that Secure Shell (SSH) uses. By default, this port is TCP port 22. This port allows the required communication for remote login. • The Bonjour service does not support IPv6 networking. To ensure that Browse Network or Search Network displays these Macs, ensure that they also have IPv4 networking enabled. IPv6 networking is supported as of 14.2.

More information

-
- [Communication ports for Symantec Endpoint Protection](#)
 - [Installing Symantec Endpoint Protection clients with Remote Push](#)
 - [Preparing for client installation](#)

Choosing a method to install the client using the Client Deployment Wizard

After you install Symantec Endpoint Protection Manager, you install the Symantec Endpoint Protection client with the Client Deployment Wizard.

Table 32: Client installation methods

Options	Description
Save Package	This installation option creates an executable installation package that you save on the management server and then distribute to the client computers. The users then install the client software, so they must have local administrator rights to their computers. You can install Windows, Mac, and Linux clients using this option. See: Installing Symantec Endpoint Protection clients with Save Package
Remote Push	Remote push installation pushes the client software to the computers that you specify. The installation begins automatically on the client computers. Remote push installation does not require the user to have local administrator rights to their computers. You can install Windows and Mac clients using this option. See: • Installing Symantec Endpoint Protection clients with Remote Push • Preparing Windows and Mac computers for remote deployment
Web Link and Email	Users receive an email message that contains a link to download and install the client software. The users then install the client software, so they must have local administrator rights to their computers. You can install Windows, Mac, and Linux clients using this option. See: Installing Symantec Endpoint Protection clients with Web Link and Email

Before you run the Client Deployment Wizard, you review the installation options, optionally customize them, and then select those options during installation. Installation options include the protection technologies to install, the installation destination folder, and the restart behavior. See:

- [Choosing which security features to install on the client](#)
- [About the Windows client installation settings](#)
- [Preparing for client installation](#)

Choosing which security features to install on the client

When you deploy the Windows client installation package with the Client Deployment Wizard, you must choose the feature set. The feature set specifies which protection features are installed on the client. You can select a default feature set or customize the feature set. Decide which feature set to install based on the role of the computers, and the level of security or performance that the computers need.

After installation, you should keep all features enabled.

Table 33: Client installation feature sets (Windows)

Feature set	Description
Full Protection for Clients	Recommended for workstations, desktop, and laptop computers. Includes all protection features. Appropriate for laptops, workstations, and desktops. Includes the full download protection and mail protocol protection. Whenever possible, use Full Protection for maximum security.
Full Protection for Servers	Recommended for servers. Includes all protection features except email scanner protection. Appropriate for any servers that require maximum network security, including the Symantec Endpoint Protection Manager server.
Basic Protection for Servers	Recommended for high-throughput servers. Includes Virus and Spyware Protection and Basic Download Protection. Since Intrusion Prevention may cause performance issues on high-throughput servers, this option is appropriate for any servers that require maximum network performance.

The Mac client installation package installs Virus and Spyware Protection and Intrusion Prevention. You cannot customize the features for the Mac client installation package.

The Linux client installation package only installs Virus and Spyware Protection.

Customizing the feature set

If you want to install a subset of the protection features, create a custom feature set. However, Symantec recommends that you install all features.

You cannot customize the features for the Mac or Linux client installation package.

To create a custom client installation feature set

1. In the console, click **Admin > Install Packages**.
2. Click **Client Install Feature Set > Add Client Install Feature Set**.
3. In the **Add Client Install Feature Set** dialog box, type a name and description, and check which protection features to install on the client.
4. Click **OK**.

More information

[How Symantec Endpoint Protection technologies protect your computers](#)

Managing client installation packages

To manage clients with Symantec Endpoint Protection Manager, you must export a managed client installation package, and then install the package files onto client computers. You can deploy the client with either Symantec Endpoint Protection Manager or a third-party deployment tool.

Symantec occasionally provides updated packages of installation files, usually when a new product version releases. You can automatically update the client software on all managed Windows and Mac clients in a group with the AutoUpgrade feature. You do not need to redeploy software with installation deployment tools.

Table 34: Client installation package-related tasks

Task	Description
Configure client installation packages	You can select specific client protection technologies to install and you can specify how the installation interacts with end users. See: • Choosing which security features to install on the client • About the Windows client installation settings
Export client installation packages	You can export packages for managed clients or unmanaged clients. You can export the packages as a single executable file or as a series of files in a directory. The method that you choose depends on your deployment method and whether you want to upgrade client software in groups. Typically, if you use Active Directory Group Policy Object, you do not choose to export to a single executable file. See: • Exporting client installation packages • How to get an unmanaged client installation package • Installing an unmanaged Windows client
Import client installation package updates	You can add updated client installation packages to the database to make them available for distribution from Symantec Endpoint Protection Manager. You can optionally export the packages during this procedure to make the package available for deployment to computers that do not have the client software. See: Importing client installation packages into Symantec Endpoint Protection Manager
Upgrade Windows and Mac clients in one or more groups	You can install the exported packages to computers one at a time, or deploy the exported files to multiple computers simultaneously. When Symantec provides updates to client installation packages, you first add them to Symantec Endpoint Protection Manager and make them available for exporting. However, you do not have to reinstall them with client deployment tools. The easiest way to update Windows and Mac clients with the latest software is to use AutoUpgrade. You should first update a group with a small number of test computers. See: Upgrading client software with AutoUpgrade You can also update clients with LiveUpdate if you permit clients to run LiveUpdate and if the LiveUpdate Settings policy permits updates.
Delete client installation packages	You can delete older client installation packages to save disk space. However, AutoUpgrade sometimes uses the older Windows client installation packages to build upgrade packages. The upgrade packages result in smaller downloads by clients.

More information

[Preparing for client installation](#)

Exporting client installation packages

You might want to export a client install package if you need those options that are not available when you use **Save Package** in the **Client Deployment Wizard**. For example, you may need to create an unmanaged client with custom policies. You may also only need either 32-bit (14.3 RU5 or earlier) or 64-bit installation packages for Windows, or need either `DPKG` or `RPM` installation packages for Linux.

Once you export the client install package, you deploy it. **Remote Push** in the **Client Deployment Wizard** can deploy the Windows and Mac packages that you export. Alternately, you can install an exported package directly on to the client, or use a third-party program to deploy it.

You can create an installation package for managed clients or unmanaged clients. Both types of packages have the features, policies, and settings that you assign. If you create a package for managed clients, you can manage them with the Symantec Endpoint Protection Manager console. If you create a package for unmanaged clients, you cannot manage them from the console. You can convert an unmanaged Windows or Mac client to a managed client at any time with **Communication Update Package Deployment** through the **Client Deployment Wizard**.

NOTE

If you export client installation packages from a remote console, the packages are created on the computer from which you run the remote console. Furthermore, if you use multiple domains, you must export the packages for each domain, or the clients do not appear in the correct domain groups.

To export client installation packages

1. In the console, click **Admin**, and then click **Install Packages**.
2. Under **Install Packages**, click **Client Install Package**.
3. In the **Client Install Package** pane, under **Package Name**, right-click the package you want to export and then click **Export**.
4. Click **Browse** to navigate to and select the folder to contain the exported package, and then click **OK**.

NOTE

Export Package does not support directories with double-byte or high-ASCII characters, and blocks their selection.

5. Set the other options according to your installation goals. The options vary depending on the type and the platform of the installation package you export.

For details about the export options in this dialog box, click **Help**.

For more information, see:

[Export Package settings](#)

6. Click **OK**.

More information

- [Importing client installation packages into Symantec Endpoint Protection Manager](#)
- [Choosing which security features to install on the client](#)
- [Restoring client-server communications with Communication Update Package Deployment](#)

Importing client installation packages into Symantec Endpoint Protection Manager

You may need to import a client installation package into Symantec Endpoint Protection Manager if you upgrade to a newer version of Symantec Endpoint Protection Manager using a database that you have restored from a previous version. The database includes older client installation packages, and you need to import the newer packages.

You should always keep the Symantec Endpoint Protection Manager version the same or later than the client version.

NOTE

You can import an executable package such as .exe or .zip file packages directly, but it is not recommended. The .info file contains the information that describes the package and ensures proper migration to future builds of the Symantec Endpoint Protection client through delta updates. On the other hand, the Symantec Endpoint Protection Manager web console does not import the .info file format. In the web console, you can only import or export packages in a single file, such as in the .zip or .exe file format.

To import client installation packages into Symantec Endpoint Protection Manager

1. Copy the installation package that you import to a directory on the computer that runs Symantec Endpoint Protection Manager.

The client installation package consists of two files. One file is named `product_name.dat`, and the other file is named `product_name.info`. These files automatically import during the installation or upgrade of Symantec Endpoint Protection Manager. You can also get the packages from the `SEPM/Packages` folder of the installation file.

2. In the console, click **Admin > Install Packages**.
3. Under **Tasks**, click **Add a Client Install Package**.
4. In the **Add a Client Install Package** dialog box, type a name and a description for the package.
5. Click **Browse**.
6. In the **Select Folder** dialog box, locate and select the `product_name.info` file for the new package you copied in step 1, and then click **Select**.
7. When the **Completed successfully** prompt appears, click **Close**.

To export the installation files and make them available for deployment, click **Export this Package**, and then complete this procedure. See:

[Exporting client installation packages](#)

After you successfully import the package, you can see a "Package is created" event in the System > Administrative log. The event is described with text similar to "Successfully imported the SEP 14.3 RU2 64-bit package by Symantec Endpoint Protection Manager. This package is now available for deployment."

Windows client installation package and content update sizes

Client installation packages, product patches, and content updates are also stored in the Symantec Endpoint Protection database and affect the storage requirements. Product patches contain information for client packages and information for each language or locale. Note that patches also create new, full client builds.

The following table displays the size of the client installation package if the maximum level of client logging and protection technologies are enabled.

Table 35: Windows client installation package size

Client type/ Definition type	*Installed with virus definitions?	64-bit package (MB)	32-bit package (MB)
Standard and Embedded CoreDefs-3**	Yes	188	175
	No	93	81
Dark network CoreDefs-1.5	Yes	288	276
	No	93	80

For more information, see:

[Choosing whether to download cloud-based or local-based definitions using the client installation type](#)

For these packages, you can set a larger heartbeat. These sizes do not include packet-level firewall logs, which are not recommended in a production environment. If client logging is disabled, and there are no new policies or content to download from the management server, the client installation package is smaller. In this case, you can set a smaller heartbeat.

* If your network has low bandwidth, install the client package without the virus definitions. As soon as the client connects to the management server, the client receives the full set of virus definitions.

All client installation packages include all features, such as Virus and Spyware, the firewall, the IPS, SONAR, System Lockdown, Application Control, Host Integrity content, and so forth. The difference between the client types are the size of the virus and spyware definitions.

Content updates require less storage space in the database and on the file system. Instead of storing multiple full revisions, the management server now stores only one full content revision plus incremental deltas. Full content updates require ~470 MB.

NOTE

You can download client patches to clients the same way as other content, using a LiveUpdate server, the management server, or a Group Update Provider. See:

[Installing Endpoint Protection client patches to Windows clients](#)

Creating custom Windows client installation packages in Symantec Endpoint Protection Manager

You can customize client installation packages for Symantec Endpoint Protection for Windows by configuring the client installation settings and the client feature sets. This customization lets you configure an installation path, the restart behavior, whether the installation package uninstalls a third-party security product, among others.

NOTE

Client Install Settings and Client Install Feature Set configurations only apply to Windows install packages. You can export a Macintosh or Linux install package through **Admin > Install Packages > Client Install Package**, but the configuration options differ.

Table 36: Tasks to create a custom Windows client installation package

Task	Details
Create a new custom client installation settings configuration	Use Client Install Settings to define the installation behavior. If you want to uninstall existing security software on your client computers, you configure it here. For more information, see: • Customizing the client installation settings • Configuring client packages to uninstall existing security software
Create a new custom feature set	Client Install Feature Sets define what protection technologies install on the client computer. See: Choosing which security features to install on the client
Create a new, custom installation package	When you export a client installation package, you select from the customized settings files you created. You also choose to where you save the package, and whether the package is a single file (.EXE) or a folder of files. You can also use the custom installation settings and the custom feature sets with the Client Deployment Wizard. For more information, see: Exporting client installation packages Installing Symantec Endpoint Protection clients with Remote Push

More information

[Preparing for client installation](#)

About the Windows client installation settings

The Client Deployment Wizard prompts you to specify the client installation settings for Windows clients. The client installation settings define the options of the installation process itself. You can define the target installation folder, whether to disable installation logging, and restart settings, among other options.

You can choose the default client installation settings, or you can add a custom **Client Install Settings** under **Admin > Install Packages > Client Install Settings**. The contextual Help provides details about the settings that you can configure.

You should use silent installations for remote deployment to minimize user disruption. When you use a silent deployment, you must restart the applications that plug into Symantec Endpoint Protection, such as Microsoft Outlook.

If you use unattended installations (**Show progress bar only**), Windows may display to users one or more pop-up windows. However, the installation should not fail even if the user does not notice them.

You should not use an interactive installation for remote deployment. This installation type fails unless the user interacts with it. Security features (such as Windows Session 0 isolation) on some operating systems may cause the interactive installation wizard to not appear. You should only use the interactive installation type for local installations. These recommendations apply to both 32- and 64-bit operating systems.

More information

- [Customizing the client installation settings](#)
- [Choosing which security features to install on the client](#)

Customizing the client installation settings

You can change the installation settings that you apply to a client installation package and for AutoUpgrade.

For example, if you want to install the client to a custom installation folder, or reset the client-server communication settings, you create custom client installation settings. You then apply this custom setting when you export or deploy a package, or set up AutoUpgrade.

To customize the client installation settings

1. In the console, click **Admin > Install Packages > Client Install Settings**.
2. Under **Tasks**, click **Add Client Install Settings**.
The default client install settings files cannot be modified.
3. Choose the operating system for which the setting file applies.
4. Enter a name and a description.
5. Make your selections from the available options on these tabs:
 - Windows: **Basic Settings** and **Restart Settings**
 - Mac: **Restart Settings** and **Upgrade Settings**Mac client restart and upgrade settings apply only to AutoUpgrade.
6. Click **OK**.

When you run the Client Deployment Wizard or configure AutoUpgrade, select the settings that you created from the drop-down menu next to **Install Settings**.

More information

- [About the Windows client installation settings](#)
- [Configuring client packages to uninstall existing security software](#)

Uninstalling existing third-party security software

You can configure and deploy new installation packages to uninstall existing security software before the installation of the Symantec Endpoint Protection client. Uninstalling existing security software allows the Symantec Endpoint Protection client to run more efficiently. You can remove existing third-party security software or an existing Symantec Endpoint Protection client.

You enable the security software removal feature by creating or modifying a custom client installation settings configuration. You then select this custom configuration during deployment.

You can use this feature to uninstall third-party security software. To see which third-party software the client package removes, see:

[Third-party security software removal in Endpoint Protection/Endpoint Security](#)

Some programs may have special uninstallation routines, or may need to have a self-protection component disabled. See the documentation for the third-party software.

You cannot remove third-party security software with Mac or Linux client packages. You must uninstall third-party security software before you deploy the Symantec Endpoint Protection client package.

NOTE

Changes to the third-party security software removal for version 14.2 means that you cannot enable it for installation packages for earlier versions. For example, you cannot enable third-party security software removal for version 14.0.1 client packages if you create them with and deploy them from Symantec Endpoint Protection Manager version 14.2.

You can also remove existing installations of Symantec Endpoint Protection that you cannot uninstall through standard methods, such as Windows Control Panel. This feature appears as a separate option in the client installation settings.

Only the packages you create using the following procedure can remove existing security software.

To configure client packages to uninstall existing security software

1. In the console, on the **Admin** page, click **Install Packages**, and then click **Client Install Settings**.
2. Under **Tasks**, click **Add Client Install Settings**.

NOTE

If you have previously created a custom client installation settings configuration, you can modify it under **Tasks**, and then click **Edit Client Install Settings**. Modifying an existing custom configuration does not modify previously exported install packages.

3. On the **Basic Settings** tab, click one of the following options:
 - **Automatically uninstall existing third-party security software**
 - To remove a corrupted version of the Symantec Endpoint Protection client, use **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled**. See: [About uninstalling the Symantec Endpoint Protection client](#)
4. Read the information about the option you chose, and then click **OK**.
You can also modify other options for this configuration. Click **Help** for more information about these options.
5. Click **OK** to save the configuration.

To deploy client packages to uninstall existing security software

1. In the console, on the **Home** page, launch the **Client Deployment Wizard**.
2. Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.
3. In the **Client Deployment Wizard**, click **New Package Deployment**, and then click **Next**.

You can use **Existing Package Deployment** to deploy install packages you previously created. However, you must have exported these packages using a custom client installation settings configuration like the one described in the previous procedure.

4. In **Select Group and Install Feature Set**, select a Windows install package. In the **Install Settings** drop-down list, select the custom client installation settings configuration that you created or modified in the previous procedure. Click **Next**.
5. Click the deployment method that you want to use, and then click **Next** to proceed with and complete your chosen deployment method.

More information

- [Choosing a method to install the client using the Client Deployment Wizard](#)
- [About the Windows client installation settings](#)
- [Preparing for client installation](#)

Choosing whether to download cloud-based or local-based definitions using the client installation type

When you specify a Windows client installation package, you must choose whether to download definitions from the cloud or locally. The cloud-enabled options include a standard client and an embedded/VDI client. Symantec Endpoint Protection also includes a dark network installation for clients that are not connected to the cloud.

NOTE

If you want to change between the Windows client installation types: **Standard client**, **Embedded or VDI**, **Dark network**, at a later time after client installation, you **must** first uninstall the existing client software, reconfigure these settings, and then reinstall the new client package.

Table 37: Download options for clients

Standard client	Dark network client	Embedded/VDI client
• Uses virus and spyware definitions in the cloud. • Installs only the latest virus and spyware definitions on disk. The standard client is approximately 80 percent to 90 percent smaller on disk than legacy standard or dark network Windows clients. • Handles AutoUpgrade with deltas rather than full installation.	• Cannot use definitions in the cloud. • Intended for clients with intermittent or no access to the cloud. • Installs the full set of virus and spyware definitions. • Similar to legacy standard-size client; uses reputation lookups for Download Insight and behavioural analysis (SONAR) if connected to the cloud. • Handles AutoUpgrade with deltas rather than full installation.	• Uses virus and spyware definitions in the cloud. • Installs only the latest virus and spyware definitions. The client is approximately 80 percent to 90 percent smaller on disk than dark network Windows clients. • The embedded/VDI client includes more size optimizations than the standard client: — The installer cache does not save after installation completes. This change means you cannot remove or modify the installation through the Control Panel unless you first copy the installation package to the client computer. — The embedded client employs NTFS compression on more folders than the standard client. • Handles AutoUpgrade with full installation packages; cannot use deltas.

More information

- [Choosing a method to install the client using the Client Deployment Wizard](#)
- [Exporting client installation packages](#)

Third-party security software removal in Endpoint Protection/Endpoint Security

The following table lists the third-party security products that the Symantec Endpoint Protection client installation package can remove. The **Automatically uninstall existing third-party security software** option in the Client Install Settings dialog box removes these products.

Security products that are not in the supported products list can be removed using the [SEPprep tool](#).

Table 38: List of third-party security products that the Client Installation Wizard removes

Version	More information
14.3 RU1 and later	Third-party security software removal in Endpoint Protection 14.3 RU1 and later
14.3 MP1	In 14.3 MP1 the Automatically uninstall existing third-party security software option was removed from the Symantec Endpoint Protection Manager. Instead, use the TPAR tool that is located in the Tools/TPAR folder of the Symantec Endpoint Protection download folder. The readme is located in: About the third-party security software removal feature in Symantec Endpoint Protection If you have a 14.3 MP1 Symantec Endpoint Protection Manager and you need to create an installation package for a 14.0 to 14.3 client, you can display and use the Automatically uninstall existing third-party security software option by adding <code>scm.uninstall.thirdparty.security.software.enabled=true</code> to the <code>conf.properties</code> file and then restart the management server service.
14.0 to 14.3	Third-party security software removal in Endpoint Protection 14

More information

- [Uninstalling existing third-party security software](#)
- [About uninstalling the Symantec Endpoint Protection client](#)

Third-party security software removal in Symantec Endpoint Security/Symantec Endpoint Protection 14.3 RU1 and later

The following table lists which third-party products and product versions that Symantec Endpoint Protection (SEP)/Symantec Endpoint Security (SES) can remove before the client installation package is installed. The client installation package removes any version of the product.

Table 39: List of third-party security products that the 14.3 RU2 and later Client Installation Wizard removes

Setting	Description
Avast	AntiVirus
AVG	AVG Internet Security Business Edition 2013
ESET	ESET Smart Security
Kaspersky	Kaspersky AntiVirus Kaspersky Endpoint Security Kaspersky Internet Security Kaspersky Security Center Network Agent

Setting	Description
McAfee	McAfee Scan Enterprise

Table 40: List of third-party security products that the 14.3 RU1 Client Installation Wizard removes

Setting	Description
Avast	AntiVirus
AVG	AVG Protection
ESET	ESET Endpoint Antivirus / ESET Endpoint Security ESET Remote Administrator Agent
F-Secure	F-Secure Anti-Spyware F-Secure Anti-Spyware Scanner F-Secure Anti-Virus Client Security Installer F-Secure Automatic Update Agent F-Secure Backweb F-Secure Browsing Protection F-Secure CustomizationSetup F-Secure DAAS2 F-Secure Device Control F-Secure Diagnostics F-Secure E-mail Scanning F-Secure FWES F-Secure GateKeeper Interface F-Secure Gemini F-Secure GUI F-Secure Help F-Secure HIPS F-Secure Internet Shield F-Secure Localization API F-Secure Management Agent F-Secure Management Extensions F-Secure NAC Support F-Secure NAP Support F-Secure NIF F-Secure Offload Scanning Agent F-Secure ORSP Client F-Secure Policy Manager Support F-Secure Protocol Scanner F-Secure Safe Banking Popup F-Secure Sidegrade Support F-Secure Software Updater F-Secure System File Update F-Secure TNB F-Secure Uninstall F-Secure Anti-Virus

Setting	Description
Kaspersky	Kaspersky Endpoint Security Kaspersky AES Encryption Module Kaspersky Anti-Virus for Windows Servers Kaspersky Security for Windows Servers Kaspersky Anti-Virus for Windows Workstations Kaspersky PURE Kaspersky Small Office Security Kaspersky AntiVirus / Kaspersky Internet Security Kaspersky Endpoint Security 8 for Windows Console Plug-in Kaspersky Anti-Virus SOS Kaspersky Security Center Network Agent
McAfee	McAfee Endpoint Security Web Control McAfee Endpoint Security Firewall McAfee Endpoint Security Threat Prevention McAfee Endpoint Security Platform McAfee Desktop Firewall McAfee VirusScan Enterprise McAfee Firewall Protection Service McAfee Virus and Spyware Protection Service McAfee Browser Protection Service McAfee SiteAdvisor Enterprise McAfee Agent McAfee Product Improvement Program McAfee Host Intrusion Prevention
Sophos	Sophos Endpoint Agent Sophos Patch Agent Sophos Network Threat Protection Sophos System Protection Sophos Client Firewall Sophos Anti-Virus Sophos Exploit Prevention Sophos Remote Management System Sophos AutoUpdate Sophos Endpoint Defense
Trend Micro	Trend Micro OfficeScan Agent

With a 14.3 MP1 and later Symantec Endpoint Protection Manager (SEPM), you can no longer create an installation package that uses the **Automatically uninstall existing third-party security software** option in the Client Install Settings dialog box. Use TPAR instead. However, if you have a 14.3 MP1 SEPM and you're creating an installation package for a SEP client older than 14.3 MP1, you can use the feature, but you have to add **scm.uninstall.thirdparty.security.software.enabled=true** to conf.properties and then restart the management server services. This action unhides the checkbox. The option only works for clients versions 14.0 to 14.3, as they still contain the client-side feature.

Restarting the client computers from the Symantec Endpoint Protection Manager

In Symantec Endpoint Protection, you may need to restart the client computers after an installation or an upgrade.

The following table describes the restart options for each of the client types.

Client type	Description
Windows	The Windows client computers restart automatically after installation by default. However, the client user can delay it until a pre-scheduled time overnight. You do not need to restart the Windows computers after you install the client software with the following exceptions: • The firewall is installed (14.3 RU1 and earlier). • Application and Device Control is installed (all 14.x versions) (14.3 RU4 and earlier). Processes that were running before you upgrade the client do not get Application Control enforcement. • Application Hardening is installed or uninstalled (14.3 RU3 and earlier). You do not need to restart the Windows computers after you upgrade the client software with the following exceptions: • You upgrade from 14.3 RU2 and earlier clients. • You install or uninstall Application Hardening. Or you upgrade from 14.3 RU3 and earlier clients that have Application Hardening. You manage Application Hardening and the clients from the Symantec Endpoint Security (SES) cloud console. • The Symantec Endpoint Protection client is installed on the same computer as the following agents: – Standalone Symantec Data Center Security – Standalone Symantec Critical System Protection – Symantec Data Loss Prevention (15.5 - 15.8) • A previous upgrade attempt from the same version failed. For example, if you unsuccessfully tried to upgrade from 14.3 RU2 to the current version. Before you export or deploy the installation package, you can configure the Windows client installation settings to customize the restart after installation. You can configure the restart options on a group to control how the client computers restart after a risk remediation or a new client download. • You can also restart the Windows client computers at any time by running a restart command from the management server. What are the commands that you can run on client computers? Running commands on client computers from the console • You can schedule the Windows client computers to restart during a time that is convenient for users. • You can force an immediate restart or let users delay the restart.
Mac	Mac client computers prompt for a restart after installation. If you push the client package and users are not logged on to the Mac computer, a hard restart occurs automatically when the installation completes. You cannot customize this setting. You can also restart the Mac client computers at any time by running a restart command from the management server. When you send a restart command to a Mac client computer, it always performs a hard restart.
Linux	Linux client computers do not require a restart and do not automatically restart after installation. You cannot restart the Linux client with a restart command from the management server.

To configure restart options on Windows client computers

1. In the console, click **Clients**.
2. On the **Clients** page, select a group, and then click **Policies**.
3. On the **Policies** tab, click **General Settings**.
4. In the **General Settings** dialog box, on the **Restart Settings** tab, select the restart method and schedule.
Some restart options apply only to Windows clients. For details, see the context-sensitive Help.

You can also add a notification that appears on the client computer before the restart occurs. The default message tells the user that a security risk remediation or a new content download requires a restart.

5. Click **OK**.

To restart a selected client computer

1. In the console, click **Clients**.
2. On the **Clients** page, on the **Clients** tab, select a group.
3. On the **Clients** tab, select a client, right-click **Run command on computers**, and then click **Restart Client Computers**.
4. Click **Yes**, specify the restart options that you require, and then click **OK**.
Some restart options apply only to Windows clients. For details, see the context-sensitive Help.

To restart the client computers in a selected group

1. In the console, click **Clients**.
2. On the **Clients** page, on the **Clients** tab, select a group, click **Run a command on the group**, and then click **Restart Client Computers**.
3. Click **Yes**, specify the restart options that you require, and then click **OK**.
Some restart options apply only to Windows clients. For details, see the context-sensitive Help.

More information

- [About the Windows client installation settings](#)
- [Preparing for client installation](#)

About managed and unmanaged (self-managed) clients

You can install the client software as a managed client or as an unmanaged client.

In most cases, you should install a managed client. Install an unmanaged client so that the user has more control over the computer, such as a test computer, or if the computer is primarily off-site. Make sure that the unmanaged client users have the appropriate level of knowledge to configure any security settings that are different from the default settings.

NOTE

You can convert an unmanaged client to a managed client at a later time by replacing the client-server communications file on the client computer. See: [Replacing the client-server communications file on the client computer](#)

Table 41: Differences between a managed and an unmanaged client

Managed client	Unmanaged client
A managed client communicates with a management server in our network. The administrator configures the protection and the default settings, and the management server downloads the settings to the client. If the administrator makes a change to the protection.	An unmanaged client does not communicate with a management server and an administrator does not manage the client.
The user doesn't have the right required to configure the client. All the settings are locked or unavailable, but we can view information about what the client does on your computer.	Client users have all the rights to configure the client and all settings.

Managed client	Unmanaged client
The administrator manages the client, but client users can change some client settings and perform some tasks. For example, client users can run your own scans and manually retrieve client updates and protection updates.	Client users can run all administrative tasks.
The administrator manages the client, but we can change all the client settings and perform all the protection tasks.	Client users manage the unmanaged client.
The managed client gets content updates from the Symantec Endpoint Protection Manager, GUPs, the Internet, and LiveUpdate.	The unmanaged client gets content updates from the Internet and LiveUpdate. The client user must update the content on each client individually.

The following table describes the differences in the user interface between a managed and unmanaged client.

Table 42: Differences between a managed client and an unmanaged client by feature area

Feature area	Managed client	Unmanaged client
Virus and Spyware Protection	The client displays a locked padlock option and the option appears dimmed for the options that you cannot configure.	The client does not display either a locked padlock or an unlocked padlock.
Proactive Threat Protection	The client displays a locked padlock option and the option appears dimmed for the options that you cannot configure.	The client does not display either a locked padlock or an unlocked padlock.
Client management and Network and Host Exploit Mitigation settings	The settings that the administrator controls do not appear.	All the settings appear.

More information

- [Checking whether the client is managed or unmanaged](#)
- [How to get an unmanaged client installation package](#)
- [Installing an unmanaged Windows client](#)

How to get an unmanaged client installation package

You can get the unmanaged Symantec Endpoint Protection client installation package in one of the following ways:

- Download a standalone client installer from the [Broadcom Support Portal](#).
- Copy a folder from within the full installation file from the [Broadcom Support Portal](#).
- Export an unmanaged client from Symantec Endpoint Protection Manager with the default policies and settings, or with custom policies and settings.

NOTE

For guidance in downloading the software, see:

[Download the latest version of Symantec Endpoint Protection](#)

To download the standalone client installer

1. Sign in to the [Broadcom Support Portal](#).
2. Download the following file:
Symantec_Endpoint_Protection_version_All_Clients_lang.zip
Where version is the version number, and lang is the language, such as EN for English.
3. Extract the contents of the file to your hard drive.

-
4. Depending on the operating system on which you want to install the client, do one of the following:
 - For Windows: Copy the 32-bit (14.3 RU5 or earlier) or 64-bit .exe file to the target computer.
 - For Mac: Copy the Mac client .zip file to the target computer.
 - For Linux: Copy the Linux client .zip file to the target computer.

NOTE

Symantec Agent or Symantec Endpoint Protection for Linux 14.3 RU1 and later cannot run as an unmanaged client.

To copy the folder from the full installation file

1. Sign in to the [Broadcom Support Portal](#).
2. Download the following file:
Symantec_Endpoint_Protection_version_Full_Installation_lang.exe
Where version is the version number, and lang is the language.
3. Double-click on the file to extract its contents.
4. Do one of the following:
 - For versions 14.2 MP1a (14.2.1023.0100) or later, the file extracts to C:\Users\username\AppData\Local\Temp\7zXXXXXXXXXX, where XXXXXXXXXX represents a random string of letters and numbers. Navigate to that folder. Do not close the installation menu.
 - For versions earlier than 14.2 MP1a (14.2.1023.0100), type or browse to a folder to extract to, and then click **Extract**. When the extraction finishes, navigate to that folder.
5. Depending on the operating system on which you want to install the client, do one of the following:
 - For Windows: Copy the folder **SEP** (32-bit) or **SEPx64** (64-bit) to the target computer.
 - For Mac: Copy the folder **SEP_MAC** to the target computer.
 - For Linux: Copy the folder **SEP_LINUX** to the target computer.

To export an unmanaged client from Symantec Endpoint Protection Manager

1. Log on to Symantec Endpoint Protection Manager.
2. Do one of the following:
 - Export an unmanaged client from Symantec Endpoint Protection Manager with the default policies and settings. See:
[Exporting client installation packages](#)
 - Export an unmanaged client from Symantec Endpoint Protection Manager with custom policies and settings. For recommendations, see:
[Recommended policies and settings for unmanaged client installation packages](#)
You cannot export an unmanaged Mac client with group policies.
You can then install the unmanaged client for Windows, Mac, or Linux.
If the file is a .zip file, you must extract all contents before you install.

More information

- [Installing an unmanaged Windows client](#)
- [About managed and unmanaged clients](#)

Installing an unmanaged Windows client

An unmanaged (or self-managed) client usually allows a user greater control of Symantec Endpoint Protection settings through the client user interface. Typically, you install an unmanaged Symantec Endpoint Protection client directly on to a Windows computer, and the installation requires user input to complete. See:

- [About managed and unmanaged clients](#)
- [How to get an unmanaged client installation package](#)

NOTE

When you install a managed Windows client installation package directly on to the client computer, the steps to install are similar. Only an **Interactive** installation requires user input. ThInstalling an unmanaged Windows cliente client installation setting options **Show progress bar only** and **Silent** do not require user input.

NOTE

Unmanaged client packages that are configured with custom policies may not display during installation some of the panels that are described. If you do not see an installation panel that the procedure step describes, skip to the next step.

To install an unmanaged Windows client

1. Run either `Setup.exe` or `Symantec_Endpoint_Protection_<versionnumber>_Win64-bit_Client_<language>.exe`, and then click **Next**.
2. On the **License Agreement Panel**, click **I accept the terms in the license agreement**, and then click **Next**.
3. On the **Setup Type** panel, click one of the following options and then click **Next**:
Click **Typical** for the most common options.
Click **Custom** to configure your installation.
 - On the **Installation Type** panel, you can choose whether to download definitions from the cloud or locally (dark network).
 - On the **Custom Setup** panel, choose which features you want to install on the computer. A red X on a feature does not install.

For more information, see: [Choosing which security features to install on the client](#)
4. If the installation wizard prompts you, click **Enable Auto-Protect** and **Run LiveUpdate**, and then click **Next**.
5. On the **File Reputation Data Submission** and **Data Collection** panels, uncheck the box if you do not want to provide pseudonymous data to Symantec, and then click **Install**.
An unmanaged client does not submit the data without a paid license, even if you leave the box checked.
6. On the **Wizard Complete** panel, click **Finish**.

More information

- [Preparing for client installation](#)
- [About the Windows client installation settings](#)

About uninstalling the Symantec Endpoint Protection client

You can uninstall the existing client installation on the client computer before the installation of Symantec Endpoint Protection begins. This feature is comparable to the CleanWipe utility, so you should not enable it for all deployments. Instead, you should only use this feature to remove corrupted or malfunctioning installations of the Symantec Endpoint Protection client.

Before you use the **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled** feature, be aware of this important information:

-
- This feature can remove all Symantec Endpoint Protection versions up to and including the version of the installation package you create.
 - This feature cannot uninstall a version of Symantec Endpoint Protection that is later than the installation package with which you include it. For example, you cannot use this feature during a planned rollback.
 - If you deploy the wrong package type with this feature enabled, it does not perform the removal. For example, if you deploy a 32-bit package to a 64-bit computer, it cannot install. Therefore, it does not remove the existing Symantec Endpoint Protection installation.
 - You cannot use this feature with an installation that uses the .MSI file directly, such as through a GPO deployment.
 - This feature does not work with a manual upgrade or AutoUpgrade. You use this feature with a fresh installation only.
 - This feature does not remove Symantec Endpoint Protection Manager.
 - This option only removes Windows LiveUpdate if no other Symantec products use it.
 - On the client computer, this feature runs silently, and does not display a status screen or user interface.
 - This option forces the installation type to **Silent**.

More information

- [Configuring client packages to uninstall existing security software](#)
- [Download the CleanWipe removal tool to uninstall Endpoint Protection](#)
- [Third-party security software removal in Endpoint Protection/Endpoint Security](#)

Uninstalling the Symantec Endpoint Protection client for Windows

You can uninstall the Windows client in the following ways:

- By using the Windows Control Panel to remove an application, typically **Programs and Features**.
- By configuring and deploying a custom client installation package that removes the Symantec Endpoint Protection client. Only use this method if uninstalling with the Windows Control Panel does not work. See: [About the Symantec Endpoint Protection client preinstall removal feature](#)
- For alternative methods to uninstall Symantec Endpoint Protection Manager and other components, see: [Uninstall Symantec Endpoint Protection](#)

If the Symantec Endpoint Protection client software uses a policy that blocks hardware devices, the policy blocks the devices after you uninstall the software. If you do not disable the device control by policy before you uninstall, use the Windows Device Manager to unblock the devices.

NOTE

Uninstalling the client does not remove it from Symantec Endpoint Protection Manager. You must also either delete the client from Symantec Endpoint Protection Manager or set up a time period to delete clients that have not connected for specified time. See:

[Deleting a client](#)

[Purging obsolete non-persistent \(NPVDI\) clients to free up licenses](#)

To uninstall the Symantec Endpoint Protection client for Windows

1. In the console, on the **Admin** page, click **Install Packages**, and then click **Client Install Settings**.
2. Under **Tasks**, click **Add Client Install Settings**.

NOTE

If you have previously created a custom client installation settings configuration, you can modify it under **Tasks**, and then click **Edit Client Install Settings**. Modifying an existing custom configuration does not modify previously exported install packages.

-
3. On the **Basic Settings** tab, check **Remove existing Symantec Endpoint Protection client software that cannot be uninstalled**.
 4. Read the message, and then click **OK**.
 5. Click **OK**.

More information

- [Uninstalling the Symantec Endpoint Protection client for Mac](#)
- [Uninstalling the Symantec Endpoint Protection client for Linux](#)

Uninstalling the Symantec Endpoint Protection client for Mac

Client users uninstall the Symantec Endpoint Protection client for Mac through the client icon on the menu bar. Uninstallation of the Symantec Endpoint Protection client for Mac requires administrative user credentials.

NOTE

After the Mac client uninstalls, the client user may be prompted to restart the client computer to complete the uninstallation. Make sure that users have saved any unfinished work and closed all open applications before they restart.

To uninstall the Symantec Endpoint Protection client for Mac

1. On the Mac client computer, open the Symantec Endpoint Protection client, and then click **Symantec Endpoint Protection > Uninstall Symantec Endpoint Protection**.
2. Click **Uninstall** again to begin the uninstallation.
3. To install a helper tool that is needed for uninstalling the Symantec Endpoint Protection client, enter your Mac's administrative username and password, and then click **Install Helper**.
4. In the **Symantec Endpoint Protection is trying to modify a System Extension** dialog box, enter your Mac's administrative username and password, and then click **OK**.

You may also be prompted to type a password to uninstall the client. This password may be a different password than your Mac's administrative password.

After the uninstallation completes, you can click **Restart Now**.

If the uninstallation fails, you may have to use an alternate method to uninstall. See:

[Uninstalling Symantec Endpoint Protection](#)

Uninstalling the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux

Run a script to uninstall the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.

NOTE

Both the Symantec Single Agent for Linux and the Symantec Endpoint Protection Linux Agent are referred to in this topic as the Linux Agent.

NOTE

For 14.3 MP1 and earlier, the Linux agent is known as the Symantec Endpoint Protection client for Linux. See below for installation instructions.

You must restore antimalware settings after you remove the SEP Linux Agent from dual agent mode. After the SEP Linux Agent uninstallation, use the DCS Manager to send DCS Antimalware configs to the agent.

To uninstall the Linux Agent (14.3 RU1 and later)

1. On the Linux computer, open a terminal application window.
2. Navigate to the following directory:
`/usr/lib/symantec/`
3. Run the following built-in script to uninstall Symantec Agent for Linux:

To remove the SEP Linux agent:

```
./uninstall.sh -u
```

or

```
./uninstall.sh -u SEPL
```

To remove the DCS agent:

```
./uninstall.sh -u DCS
```

To remove both agents (SEP Linux and DCS):

```
./uninstall.sh -u ALL
```

4. Reboot the computer after the uninstallation finishes and the reboot prompt appears.

The `uninstall.sh` script removes all of the Linux components (`sdcss-caf`, `sdcss-sepagent`, and `sdcss-kmod`).

```
[root@localhost symantec]# ./uninstall.sh
Running ./uninstall.sh (PWD /usr/lib/symantec; version 2.2.4.41)
Uninstalling Symantec Agent for Linux (SEPM) ...
Removing packages sdcss-caf sdcss-sepagent sdcss-kmod sdcss-scripts
Symantec Agent for Linux (SEPM) uninstalled successfully.
A reboot is required to complete uninstallation.
Please reboot your machine at the earliest convenience.
```

To uninstall the Symantec Endpoint Protection client for Linux (14.3 MP1 and earlier)

You must have superuser privileges to uninstall the Symantec Endpoint Protection client on the Linux computer. The procedure uses `sudo` to demonstrate this elevation of privilege.

1. On the Linux computer, open a terminal application window.
2. Navigate to the Symantec Endpoint Protection installation folder with the following command:

```
cd /opt/Symantec/symantec_antivirus
```

The path is the default installation path.

3. Use the built-in script to uninstall Symantec Endpoint Protection with the following command:

```
sudo ./uninstall.sh
```

Type your password, if prompted.

This script initiates the uninstallation process.

4. At the prompt, type `Y` and then press **Enter**.

Uninstallation completes when the command prompt returns.

NOTE

On some operating systems, if the only contents of the `/opt` folder are the Symantec Endpoint Protection client files, the uninstaller script also deletes `/opt`. To recreate this folder, enter the following command:

```
sudo mkdir /opt
```

To uninstall using a package manager or software manager, see the documentation specific to your Linux distribution.

Deleting a client

When you delete a client computer, you must also uninstall the client software.

If you do not also uninstall the client, the management server continues to download content updates to the client computer. You can also set up a time period to delete clients that have not connected for specified time. See:

[Uninstalling the Symantec Endpoint Protection client for Windows](#)

[Purging obsolete non-persistent \(NPVDI\) clients to free up licenses](#)

To delete a client

1. In the console, on the **Clients** page, select the group that the client is in.
2. Right-click the client and click **Delete** and then **Yes**.

Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection (SEP)

Update to the latest release of Symantec Endpoint Protection Manager and the clients.

Use this topic to upgrade to the latest release of SEP and take advantage of the new features. This information is specific to upgrading the software in environments where a compatible version of the product is already installed.

Before you upgrade, review the following information:

- [Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)
- [Known issues and workarounds](#)
- [What's new for all releases of Symantec Endpoint Protection 14.x](#)
- [Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection 14.x](#)

Table 43: Process for upgrading Symantec Endpoint Protection

Task	Description
Step 1: Download the latest version from the Broadcom Download Center	For links and information, see: Download the latest version of Symantec software Before you upgrade the Symantec Endpoint Protection Manager (SEPM) and the Symantec Endpoint Protection clients, make sure you maximize the protection of your network during the upgrade by following these best practices: • Symantec recommends that you do not perform third-party installations simultaneous to the upgrade of Symantec Endpoint Protection. Installing third-party software that makes network- or system-level changes may cause undesirable results when you upgrade Symantec Endpoint Protection. • If possible, restart client computers before installing or upgrading Symantec Endpoint Protection. • Symantec recommends that you upgrade the entire network to the current version of Symantec Endpoint Protection, rather than manage multiple versions. For more information, see: Upgrade best practices for Endpoint Protection 14.x
Step 2: Back up the database and prepare for disaster recovery	Back up the database, logs, and recovery file that Symantec Endpoint Protection Manager uses to ensure the integrity of your client data. These steps are different depending on your version. See: Disaster recovery best practices for Endpoint Protection
Step 3: Stop the Symantec Endpoint Protection Manager service	You must manually stop the management server service on all sites before you install a newer version. The management server service stops the Syslog service or similar service that runs on the SEPM and which could potentially lock SEPM files or folders and cause the upgrade to fail. After you upgrade, the management server automatically starts the service. Note: If the management server replicates with other management servers, make sure that replication does not occur during the period that you upgrade the SEPM and that the management server service is stopped. See: Preventing replication during an upgrade

Task	Description
Step 4: Upgrade the Symantec Endpoint Protection Manager software	Install the new version of Symantec Endpoint Protection Manager over the existing version on all sites in your network. The existing version is detected automatically, and all settings are saved during the upgrade. See: • Upgrading a management server • Installing Symantec Endpoint Protection Manager If you enrolled a Symantec Endpoint Protection Manager domain with the SES cloud server (hybrid management) before the upgrade, the domain remains enrolled during the upgrade process. You can also enroll any domain after the upgrade. See: Enrolling a domain in the cloud console from the Symantec Endpoint Protection Manager
Step 5: Upgrade Symantec client software	You do not need to uninstall previous clients before you install the new version. The over install process saves the client settings, and then upgrades the client to the latest version. You should first update a group with a small number of test computers before you update your entire production network. If you use clients as Group Update Providers, you must upgrade them first. See: Upgrading Group Update Providers Review the applicable steps in the following topics: • Preparing for client installation • Preparing Windows and Mac computers for remote deployment Then choose from one of the available methods to upgrade clients: • AutoUpgrade: AutoUpgrade is the easiest way to update the Windows and Mac client software in groups. You assign client packages to groups in the management server, either manually or by using the Upgrade Clients with Package wizard. No further action is required on your part to complete the upgrade process. See: Upgrading client software with AutoUpgrade AutoUpgrade does not support the Symantec Agent for Linux 14.3 RU1. • Installation file: Download the client installation file from the Broadcom Download Center. For links and information, see: Download the latest version of Symantec software • Client Deployment Wizard: Run the Client Deployment wizard in the management server. This wizard walks you through the creation of a client package that can be deployed by a web link and email, remote push, or saved for a later local installation. You can also deploy using third-party tools. See: Choosing a method to install the client using the Client Deployment Wizard

Upgrade best practices for Endpoint Protection 14.x

When upgrading, follow the recommended best practices and be aware of any potential issues and risks.

The following resources help you to plan and perform an optimal upgrade to the current version of Symantec Endpoint Protection (SEP):

- [Benefits of upgrading to the latest version](#)
- [Important information for the latest version](#)
- [Things to know before getting started](#)
- [Best practices](#)
- [Frequently asked questions \(FAQ\)](#)

Benefits of upgrading to the latest version

To get the latest security features, operating system support, and customer fixes, upgrade to the latest version. For information on what features each version offers, see:

What's new for all releases of Symantec Endpoint Protection (SEP) 14.x

Important information for the latest version

Table 44: Important information for the latest version

System requirements and release notes	Review the following carefully before you upgrade: Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security Before the upgrade, use the Symantec Diagnostic tool to determine whether the computers meet minimum system requirements. See: Download SymDiag to detect product issues If you plan to upgrade your operating system, be sure to first upgrade Symantec Endpoint Protection to a version that supports the operating system. Leaving an unsupported version of Symantec Endpoint Protection in place when you upgrade the operating system can have unexpected results.
Supported and unsupported upgrade paths	Make sure that the currently installed version can be migrated or upgraded to the new version. Review the following: • Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection
Important installation and upgrade information	• When you upgrade from a Symantec Endpoint Protection Manager embedded database to a default Microsoft SQL Server Express database (14.3 RU1 and later), the following error may appear: <code>The specified password does not meet strong password requirements</code>. To work around this issue, see: While upgrading a SEPM embedded database to 14.3 RU1 the error "The specified password does not meet strong password requirements" • Symantec Endpoint Protection 14.3 RU2 clients cannot be managed by a 14.3 RU1 MP1 or earlier Symantec Endpoint Protection Manager. • For an upgrade to 14.3 RU1 or later, the default Microsoft SQL Server Express database replaces the embedded database. The maximum database size is 10 GB. • For an upgrade to 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if some default names have been changed. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected. If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add. These actions prevent any issues with IPv6 communications. • You cannot upgrade legacy Symantec Endpoint Protection clients to version 14.2 or later if the network only uses IPv6 communications. In this context, legacy clients are Symantec Endpoint Protection clients with a version earlier than 14.2. These earlier client versions do not support IPv6 communication, so the upgrade can result in communication issues with Symantec Endpoint Protection Manager. Upgrade the clients to version 14.2 or later before moving the environments to a pure IPv6 network. Alternately, uninstall the legacy versions, then deploy a new 14.2 or later package to these client computers. • If Symantec Endpoint Protection uses a SQL Server database and your environment only uses TLS 1.2, ensure that SQL Server supports TLS 1.2. You may need to patch SQL Server. See: TLS 1.2 support for Microsoft SQL Server This recommendation applies to SQL Server 2008, 2012, and 2014. • New installations of Symantec Endpoint Protection Manager enable secure communications between the clients and the management console. The upgrade maintains current communication configuration.

Things to know before you get started

The following table lists the recommended routine maintenance tasks you should perform before you upgrade. Maintenance may include disk error checks, defragmentation of the hard drive, or other routine health checks.

Table 45: Recommended routine maintenance tasks

Insufficient disk space	Ensure that the management server has enough disk space to perform the upgrade. For a successful Symantec Endpoint Protection Manager upgrade, free space should be at least three times the size of the database. Consult the system requirements for the free space that is required to install the Symantec Endpoint Protection client. See: Increasing Symantec Endpoint Protection Manager available disk space before an upgrade.
Proxy servers	Ensure that you have made the proper exclusions to any peripheral firewall or proxy to ensure successful communication with all Symantec servers. See: URLs that allow SEP and SES to connect to Symantec servers
Scanning exclusions	You may need to create additional scanning exclusions before you deploy the client upgrade. See: • What scan exclusions should be applied to all Windows clustered server nodes? • About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products • Best practices for virtualization • Excluding known risks from virus and spyware scans on Windows clients
Steps to upgrade	For general information on upgrading Symantec Endpoint Protection, see: Upgrading and Migrating to the Latest Release of Symantec Endpoint Protection (SEP)
Upgrading unsupported languages	When you upgrade the SEPM from a non-supported language, SEPM automatically upgrades to English (14.3 RU2 and later). If you want to upgrade to a different supported language, such as from Italian to French, before you upgrade, see: Upgrading Symantec Endpoint Protection Manager 14.3 RU2+ to a supported language To upgrade an unsupported language on the Windows client, see: Upgrading client software with AutoUpgrade Both the Symantec Endpoint Protection Manager (SEPM) and the clients are translated into the following languages: • In 14.3 RU2 and later: English, Brazilian Portuguese, French, Japanese, and Spanish. • In 14.3 RU4 and later: Simplified and Traditional Chinese. • In 14.3 RU5 and later: Czech, Polish, and Russian.

Best practices

Table 46: Best practices

Back up before you upgrade	As a best practice, always back up the Symantec Endpoint Protection Manager database before an upgrade. See: Backing up the database and logs
AutoUpgrade	Use the Upgrade Clients with Package wizard to upgrade existing Windows and Mac clients. You may want to schedule AutoUpgrade for after hours, due to possible bandwidth usage. You can stage client packages on a web server, and then run Upgrade Clients with Package . There are alternate methods to deploy the upgrade package as well, such as through the Client Deployment Wizard. See: Upgrading client software with AutoUpgrade

Fresh install of Symantec Endpoint Protection Manager	You can use the Communication Update Package to connect existing clients to a new installation of the Symantec Endpoint Protection Manager. For example, if you decommission an existing server, and install Symantec Endpoint Protection Manager to a new server instead. Create a new client installation setting that resets client-server communications settings, and then deploy the Communication Update Package in the same way as clients: Help > Getting Started Page > Install the client software on your computers. You can also reset the client-server communications settings for Mac computers with a client installation setting. After the clients are connected, you can upgrade the clients with AutoUpgrade. See: About the Windows client installation settings
Virtualization	The Symantec Endpoint Protection clients can be used to protect virtual instances of the supported operating systems. Symantec Endpoint Protection Manager can be installed and managed on virtual instances of the supported operating systems. Symantec Endpoint Protection includes additional management options for virtual clients, such as Shared Insight Cache and a separate configuration option for purging offline non-persistent GVMs. See: Best practices for virtualization in Symantec Endpoint Protection
Disaster recovery preparation	Before you begin the upgrade, ensure that you have backed up the current Symantec Endpoint Protection Manager installation using disaster recovery preparation techniques. If the upgrade then fails, you can restore the Symantec Endpoint Protection Manager to functionality more quickly. To recover an installation after a failure, due to database schema and other changes, you must reinstall using the exact version previously in use. See: See Disaster recovery best practices for Endpoint Protection

Frequently asked questions (FAQs)

Q: Where do I get the current version of Symantec Endpoint Protection?

A: From the Broadcom Support Portal. See the following page for guidance:

[Download the latest version of Symantec software](#)

Contact Technical Support for additional assistance:

[Symantec Endpoint Security](#)

Q: How do I activate my license?

A: After you log on to Symantec Endpoint Protection Manager, click **Help > Getting Started Page**, under **Required Tasks**.

Q: What are the upgrade methods? When should each method be used?

A: There are many methods available to upgrade clients. Second, decide which method is most appropriate for the situation. Every situation is different, so Symantec provides many different methods for accomplishing this goal:

- AutoUpgrade: Assign client packages to groups in the management console, either manually or by using the **Upgrade Clients with Package** wizard.
- Local installation from the installation file or installation media.
- Run the Client Deployment Wizard from the management console. The Client Deployment Wizard walks you through the creation of a client package. You can then choose to deploy by emailing a web link to users, by a remote push. You can also save the package for local installation or with a third-party deployment tool.

Before you begin, ensure the client computers are ready to receive an upgrade package. See:

[Managing the Symantec Endpoint Protection client installation](#)

Q: What's the recommended migration order? What do I upgrade first in my environment?

A: The recommended order is to upgrade is as follows:

1. Symantec Endpoint Protection Managers
2. Group Update Providers
3. The remaining clients as needed

Q: How can I generate a list of Symantec Endpoint Protection versions installed in my environment?

A: Generate this list using **Reports**. See:

[Generating a list of the Symantec Endpoint Protection versions installed in your network](#)

Q: What happens if my version of Symantec Endpoint Protection reaches End of Service (EOS)?

A: If your version of Symantec Endpoint Protection is no longer supported, you should upgrade to a later version. For information on which versions have reached the EOS, see: [Product Lifecycle - Cyber Security Software](#)

Upgrade resources for Symantec Endpoint Protection

Table 47: Upgrade resources

Item	Resource
Client installation package settings and features	You can configure client installation packages with a variety of settings and protection features. See: • Symantec Endpoint Protection features based on platform • About the Windows client installation settings • Choosing which security features to install on the client
Feature and policy descriptions	For more information, see: • How Symantec Endpoint Protection technologies protect your computers • The types of security policies
Feature dependencies	For more information, see: Symantec Endpoint Protection feature dependencies for Windows clients
Manage product licenses	Symantec Endpoint Protection is licensed according to the number of clients that are needed to protect the computers at your site. See: Symantec Endpoint Protection product license requirements
Additional resources	See the following articles: • Upgrade best practices for Endpoint Protection 14.x • Download the latest version of Symantec software • Release notes, new fixes, and system requirements for all versions of Endpoint Protection

More information

[Upgrading to a new release](#)

Upgrading Windows client computers to 14.3 RU8 and later with Microsoft Azure Code Signing (ACS) support

Find out why Symantec is adopting Microsoft Azure Code Signing and how that affects your 14.3 RU8 and later upgrade or installation.

When you upgrade or install Symantec Endpoint Protection 14.3 RU8, the client user may see the following error message: Symantec Endpoint Protection can only be installed on systems with Azure Code Signing support. You must install the appropriate Windows security update for this system.

This message appears because the Symantec Endpoint Protection installer detects that the computer does not run a version of Microsoft Windows that supports Microsoft Azure Code Signing. The Symantec Endpoint Protection client blocks the installation of 14.3 RU8 and later clients until the computer has the ACS support installed.

What is Microsoft Azure Code Signing and why is Symantec adopting it?

Microsoft helps developers use their toolsets to build and distribute applications securely by using Azure Code Signing. ACS establishes the identity of the publisher of an application and the integrity that it has not been modified since publication.

Microsoft requires security vendors to sign binaries using ACS. ACS support must be present on the client computer operating system for the Symantec Endpoint Protection client to run successfully. The Symantec Endpoint Protection client 14.3 RU8 has binaries that are signed using the Microsoft Azure Code Signing infrastructure. Symantec Endpoint Protection checks whether ACS is already supported on the operating system before you install or upgrade. If not, you are required to either [install ACS support](#) or upgrade to Windows 10 21H2 or later.

NOTE

14.3 RU7 and earlier client computers are not affected until you upgrade to 14.3 RU8 or later.

More information:

- [Azure Code Signing, democratizing trust for developers and consumers](#)
- [KB5022661—Windows support for the Azure Code Signing program](#)

Installing ACS support on the client computer

Microsoft includes the ACS support for Windows 10 21H2 automatically, but not for Windows 10 21H1 and earlier versions.

To install ACS support on the Symantec Endpoint Protection client computer

1. Check which client computers run Windows 10 21H1 or earlier.
2. Do either one of the following tasks:
 - Upgrade the client computer to run a Windows 10 21H2 or later release, which already includes the ACS support.
 - [Manually install](#) the Microsoft security update [for the operating system](#) that each client computer runs.
3. Retry the Symantec Endpoint Protection client upgrade.

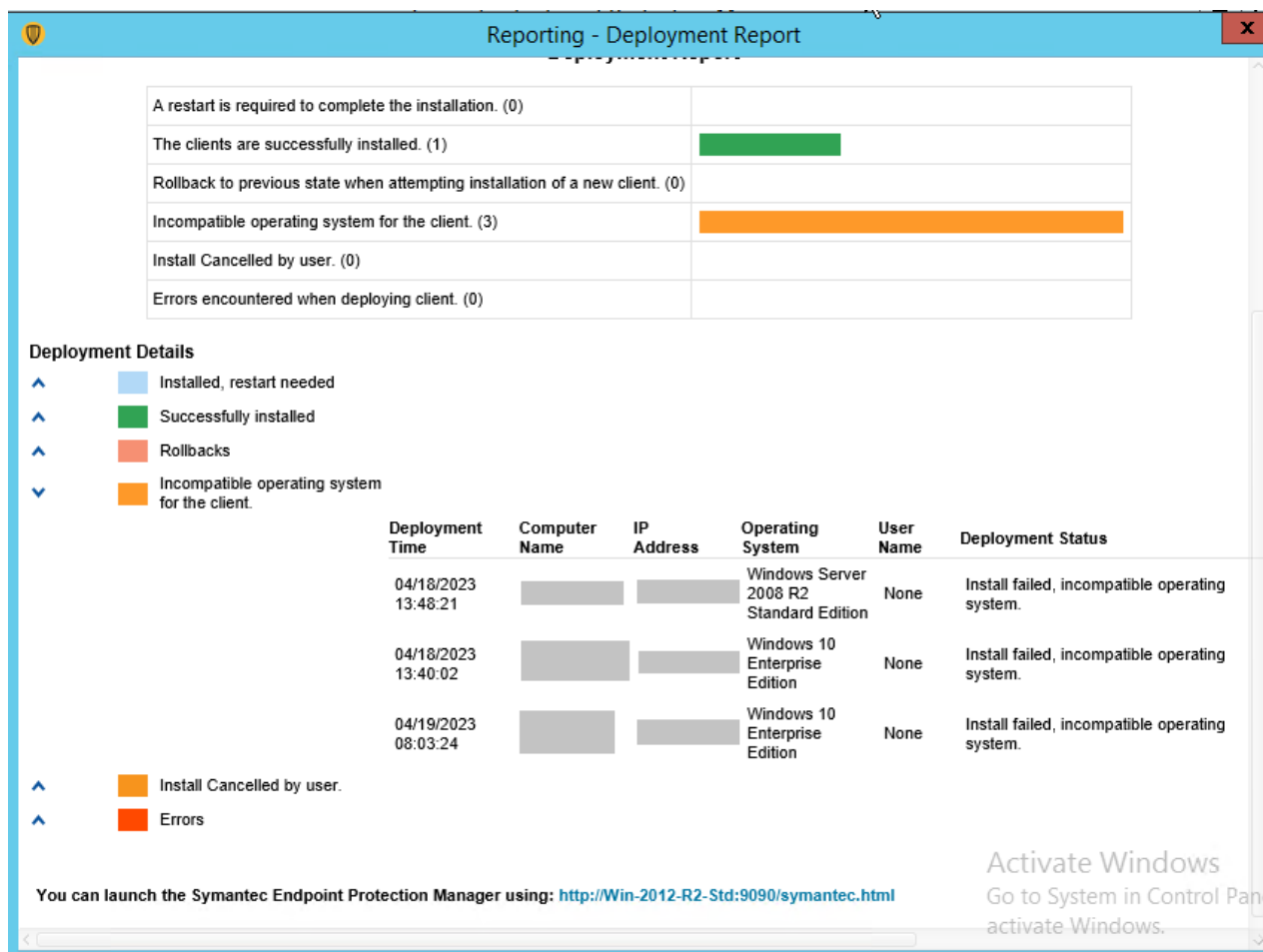
Checking which client computers support and do not support ACS

You can find which client computers already have ACS support installed on either the on-premises Symantec Endpoint Protection Manager (SEPM) or the Symantec Endpoint Security (SES) cloud console.

In the Symantec Endpoint Protection Manager:

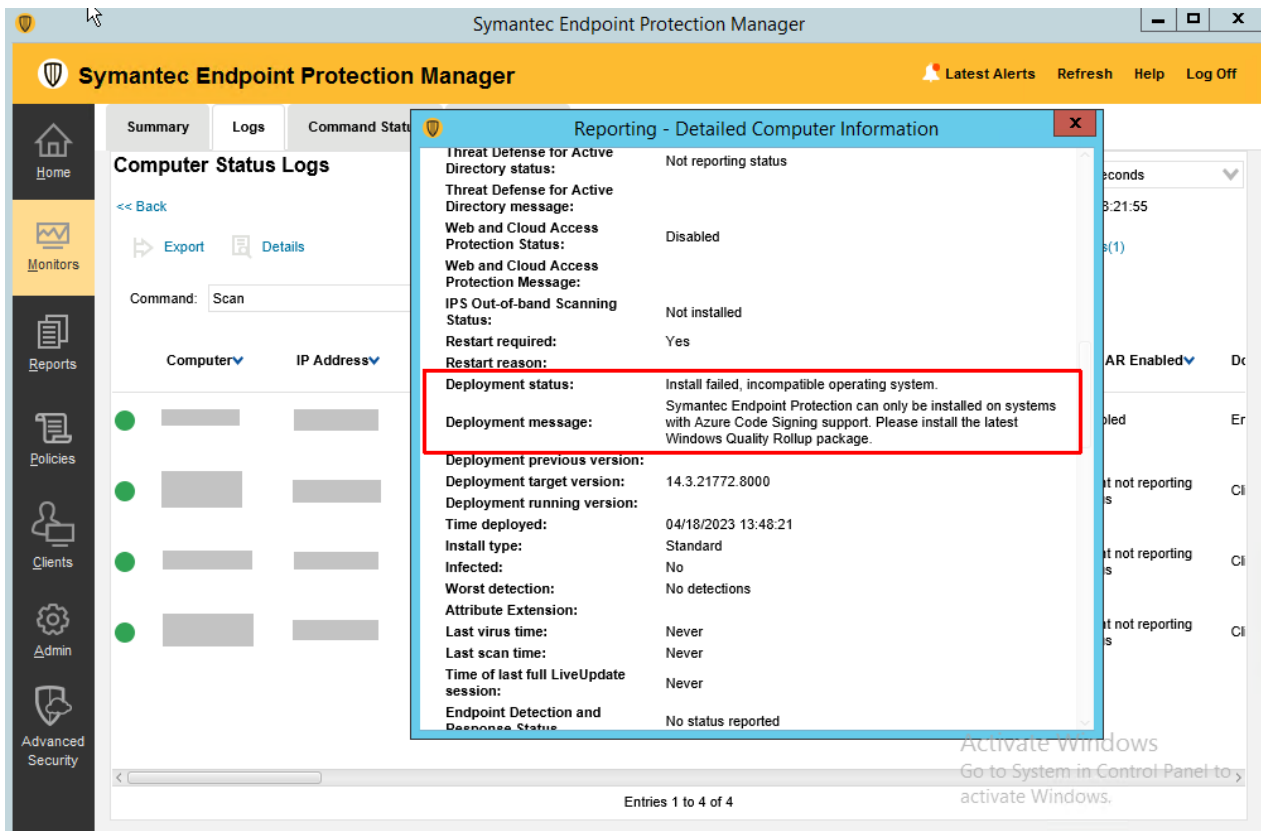
Use any of the following methods.

- In the console, create a Quick Report for the deployment status. In the **Deployment Status** column, look for clients with the following status: `Install failed`; `Incompatible operating system`



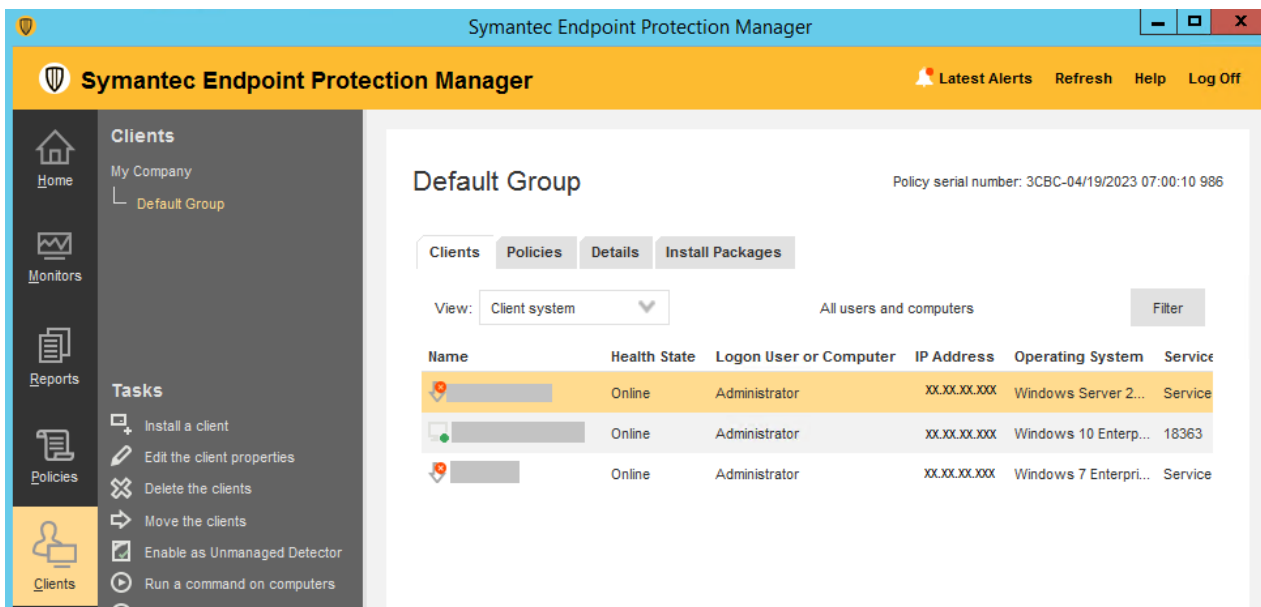
For more information, see: [Running a report on the deployment status of clients](#)

- In the Computer Status log, look for entries in the **Operating System** column for the following status: Install failed; Incompatible operating system



For more information, see: [Running and customizing quick reports](#)

- In the console, click **Clients** > **Clients**. In the **Name** column, look for the clients with a red icon that indicates a failed installation.



For more information, see: [Checking whether the client is connected to the management server and is protected](#)

In the Symantec Endpoint Security cloud console:

- In the cloud console, on the **Devices** page > **Device Groups** tab, select the **Activity History** tab. In the **Description** column, look for any devices with the following status:
 - A client upgrade package failed to install. Error: Install script executable failed.
 - A LiveUpdate session encountered errors. Error: Install script executable failed.
 - An update for Symantec Endpoint Protection WIN64 from LiveUpdate failed to install.

In the Symantec Endpoint Protection client:

- In the Symantec Endpoint Protection client System log, look for the following error message:
Symantec Endpoint Protection can only be installed on systems with Azure Code Signing support. You must install the appropriate Windows security update for this system.

Windows operating systems with ACS support

Microsoft has security updates for most Windows operating systems that the Symantec Endpoint Protection client runs on.

Support for Azure Code Signing was made available in the operating system versions starting with the releases listed in the following table. [Select the KB number](#) and download the security update for each affected client computers in your network to allow a successful Symantec Endpoint Protection client 14.3 RU8 and later installation or upgrade.

NOTE

If your operating system is not listed in the table below, contact Microsoft.

Table 48: Windows operating systems that have either native ACS support or updates

Operating system	KB number
Windows Server 2022	5005619
Windows Server 2019	5005625
Windows Server 2016	5022661
Windows Server 2012 R2	5006729
Windows 11 22H2 ARM Windows 11 22H2 Windows 11 21H2 Windows 11 21H1	Not needed; ACS support is native to the operating system.
Windows 10 22H2 Windows 10 21H2	Not needed; ACS support is native to the operating system.
Windows 10 21H1 Windows 10 20H2 Windows 10 2004	5005611
Windows 10 1909	5005624
Windows 8.1	5006714

NOTE

Microsoft does not provide ACS updates for Windows 7/Windows 8/Windows Embedded. Starting on September 26, 2023, Symantec content updates are no longer signed with an SHA-1 certificate, which affects Windows Vista/Windows 7/Windows Server 2008/Windows 2008 R2. S

For more information, see: [Endpoint Protection Content Delivery Changes for Windows Vista, 7, Server 2008 and 2008 R2](#)

Manually installing the Microsoft security updates for ACS

If the client computers are not set up to install security updates automatically, you must manually install the Microsoft Servicing Stack Updates followed by the Microsoft security update that includes the ACS support.

NOTE

The client computer must also have the [Microsoft Identity Verification Root Certificate Authority 2020](#) certificate authority that is installed in the Cert Store (Trusted Root CA list). If the computer has internet access and Windows Update is enabled, this certificate authority should get downloaded automatically.

Step 1 : Install the Microsoft Servicing Stack Updates

After the client users install a Windows security update, they may see a message that states that the update does not apply to their operating system. This message can appear if the correct Windows Service Stack Update did not get installed. This message can also appear if the content in the C:\Windows\SoftwareDistribution\Download folder is too large.

if you see this message, you must install the latest Microsoft Servicing Stack Updates before you install the ACS security updates, .

For information on Servicing Stack Updates, see:

- [Servicing Stack Updates](#)
- [Windows Update Troubleshooter](#)

Step 2: Install the Microsoft security updates

1. From the Microsoft KB security update page, download the security update that is associated with the operating system for each client computer.

For more information, see:

[KB5022661—Windows support for the Azure Code Signing program](#)

2. Install the security update.

Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection

Generally, for Symantec Endpoint Protection versions earlier than the latest version, every version on the list before it is supported. However, you should confirm by referring to the release notes for your specific version. See:

[Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection](#)

See also: [Upgrade best practices for Endpoint Protection 14.x](#)

Symantec Endpoint Protection client for Windows

The following versions of the Symantec Endpoint Protection Windows client can upgrade directly to the current version:

- All releases of 14.x, 14.2.x, and 14.3.x

Symantec Endpoint Protection client for Mac

The following versions of the Symantec Endpoint Protection client for Mac can upgrade directly to the current version:

- All releases of 14.x, 14.2.x, and 14.3.x (14.3 RU7 was not released).
The Symantec Endpoint Protection client for Mac was not updated for 14.0.1 MP2.

Symantec Single Agent for Linux

NOTE

As of version 14.3 RU1, the Linux client installer detects and uninstalls earlier versions of the Linux client, and then performs a fresh install of the new client. Old configurations are not retained.

The following versions of the Symantec Endpoint Protection client for Linux can upgrade directly to current version:

- All releases of 14.x, 14.2.x, and 14.3.x (14.3.7 was not released).

In 14.3 RU1, the Symantec Endpoint Protection client for Linux was renamed to the Symantec Single Agent for Linux.

If you have a build number but you are not sure how it translates to release version, see:

[About Endpoint Protection release types and versions](#)

Unsupported upgrade paths

You cannot migrate to Symantec Endpoint Protection from all Symantec products. You must uninstall the following products before you install the Symantec Endpoint Protection client.

- Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.3 RU8 to 14.3 RU7, you must first uninstall Symantec Endpoint Protection 14.3 RU8.
- 14.3 RU6 and later does not support 32-bit operating systems. Either upgrade your computers to a 64-bit operating system or install 14.3 RU5 for 32-bit operating systems.
- 14.0.x dropped support for Windows XP, Server 2003, and any Windows Embedded operating system that is based on Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 can manage these computers as legacy 12.1.x clients, although 12.1.x clients are EOL. For these clients, you may want to use a Symantec product that still supports these legacy operating systems, such as Data Center Security (DCS).
- All Symantec Norton products
- Symantec Endpoint Protection for Windows XP Embedded 5.1

Supported paths to the Symantec Endpoint Security cloud console

For the hybrid option:

- *Symantec Endpoint Protection Manager*: Symantec recommends the latest version but a minimum of 14.3 MP1 (14.3.1169.0010).
- *Symantec Endpoint Protection client*: Version 14.3 MP1 (14.3.1169.0010) or later. The client runs on Windows Server 2008 R2 or later and not Windows Server 2008 RTM/SP1/SP2.

See: [Migrating to the SES cloud console](#)

Increasing Symantec Endpoint Protection Manager available disk space before an upgrade

The Symantec Endpoint Protection Manager installation requires a minimum amount of available disk space. Make sure that any current servers or new hardware meet the minimum hardware requirements. However, additional available disk space may be needed during an upgrade to allow for the creation of temporary files.

Make a backup of the database before making configuration changes. See:

[Backing up the database and logs](#)

Table 49: Tasks to increase disk space on the management server

Task	Description
Change the LiveUpdate settings to reduce space requirements	1. Go to Admin > Servers and right-click Local Site. Select Edit Site Properties. 2. On the LiveUpdate tab, reduce the number of content revisions to keep. For an upgrade, you can lower the setting to 10. Allow time for Symantec Endpoint Protection Manager to purge the extra revisions. However, the reduction of revision numbers may trigger full update downloads from the clients that check in. An increase in these full update requests may negatively affect network performance. Note: Returning the revision setting to its previous value after the upgrade completes is not necessary. Improvements to the way Symantec Endpoint Protection Manager stores and manages content means that a larger number of revisions takes up less disk space than in earlier versions. For more information, see: • How to update content and definitions on the clients • Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager
Make sure that unused virus definitions are deleted from the Symantec Endpoint Protection Manager database	1. Go to Admin > Servers, right-click the database server, and then select Edit Database Properties. The database name is SQLEXPRESSSYM (14.3 RU1 and later) or localhost (143 MPx and earlier). For a Microsoft SQL Server database, the database server name varies based on the location of your database. 2. On the Log Settings tab, under Risk Log Settings, make sure that Delete unused virus definitions is checked.
Relocate or remove co-existing programs and files	• If other programs are installed on the same computer with Symantec Endpoint Protection Manager, consider relocating them to another server. You can remove unused programs. • If storage-intensive programs are installed on the same computer with Symantec Endpoint Protection Manager, consider dedicating a computer to support only Symantec Endpoint Protection Manager. • Remove temporary Symantec Endpoint Protection Manager files. For a list of temporary files that you can remove, see the article: Symantec Endpoint Protection Manager directories contain many .TMP folders consuming large amounts of disk space Note: Defragment the hard drive after removing programs and files.
Use an external database	If the Symantec Endpoint Protection database resides on the same computer with Symantec Endpoint Protection Manager, consider installing a Microsoft SQL Server database on another computer. Significant disk space is saved and in most cases, performance is improved. See: About choosing a database type

NOTE

Make sure that the client computers also have enough disk space before an upgrade. Check the system requirements and as needed, remove unnecessary programs and files, and then defragment the client computer hard drive. See:

[Low disk space on a Symantec Endpoint Protection Manager](#)

Upgrading the management server

You must upgrade all management servers before you upgrade any clients.

If you upgrade management servers in an environment that supports load balancing, failover, or replication, you must prepare and upgrade them in a specific order.

WARNING

You must follow the scenario that applies to your type of installation, or your upgrade can fail.

Table 50: Upgrade tasks

Task	Description
Upgrade the management server	Review the system requirements and supported upgrade paths, upgrade the management server, and then configure it with the Management Server Configuration Wizard. The following applies to a Symantec Endpoint Protection Manager upgrade: - Windows Server 2008, all desktop operating systems, and 32-bit operating systems are no longer supported. - SQL Server 2014 is the minimum release supported for the database. Note: You may need to edit the domain security policies to allow the virtual service accounts to run correctly for Windows 7 / Server 2008 R2 or later. See: Error: "...services require user rights" or "...cannot read the user rights" during installation or configuration Note: You are not required to restart the management server computer after the upgrade, but you may notice performance improvements if you do. For more information, see: Installing Symantec Endpoint Protection Manager Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x
Log onto the management server	When the Symantec Endpoint Protection Manager logon panel appears, you can log on to the console by using your logon credentials. See: Logging on to the Symantec Endpoint Protection Manager console

More information

- [Setting up failover and load balancing](#)
- [Setting up sites and replication](#)

Best practices for upgrading from the embedded database to the Microsoft SQL Server Express database

In 14.3 RU1, the default database that is installed with Symantec Endpoint Protection Manager (SEPM) changed from the embedded database to the Microsoft SQL Server Express 2017 database. When you upgrade or install the management server for the first time using the default configuration in the Management Server Configuration Wizard, the SQL Server Express database is installed automatically and replaces the embedded database.

When you upgrade to version 14.3 RU1 or later, the management server computer must fulfill certain requirements, or the management server upgrade cannot proceed. The Management Server Configuration wizard informs you if you encounter these issues and gives you the opportunity to fix them.

Things to know before you upgrade

Before the upgrade, check the following issues that you may need to fix before you install.

Table 51: Fixing issues before upgrading

Issue	Description
Insufficient database size	The SQL Server Express database has a maximum capacity of 10 GB for data files and log data. The Symantec Endpoint Protection Manager makes a backup of the embedded database before the installation starts. If that backup is larger than 10 GB, the upgrade cannot continue. You must reduce the amount of data either before you start the upgrade or during the upgrade. The Management Server Configuration wizard informs you when the database size is too large. If the database is over 10 GB before you start the installation, perform the following tasks: Reducing the database size when the database is full before an upgrade to Microsoft SQL Server Express Both the Microsoft SQL Server Express database and the Microsoft SQL Server database use a feature called FILESTREAM to reduce the database size. If you find out that the database size is too large or close to too large during the upgrade, you can perform the following actions: Enabling FILESTREAM for the Microsoft SQL Server database Note: If you use the SQL Server database, periodically check the database size to make sure that the database does not reach its maximum size. See: Increasing the Microsoft SQL Server database file size
Insufficient disk space	Ensure that there is a minimum of 10 GB of available disk space on the management server computer to perform the upgrade. See: Making more disk space available to upgrade to the default Microsoft SQL Server Express database
The Symantec Endpoint Protection Manager does not communicate with the database	Symantec Endpoint Protection Manager uses a certificate to authenticate communications between the Symantec Endpoint Protection (SEPM) and the Microsoft SQL Server Express or SQL Server databases. You must generate the certificate and import it into the Symantec Endpoint Protection Manager computer for SEPM to connect to either the SQL Server database. If the certificate does not exist, is expired, or is about to expire, the connection between SEPM and the database fails. See: Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server To check that the management server connects to the database, see: Verifying the management server connection with the database
Troubleshooting issues with upgrading to the Microsoft SQL Server Express	You may have one of the following issues when you upgrade: • The Windows update is out of date or the Windows update service is not running. To troubleshoot this issue, cancel the SEPM installation, run the latest update or restart the Windows update service, restart your computer, and then continue the Symantec Endpoint Protection Manager installation. • The SQL Server Express database does not install. To troubleshoot, review the database logs. See: Troubleshooting Installation issues with the Endpoint Protection Manager's Default SQL Server Express database • No connection between the Symantec Endpoint Protection Manager and the database. See: – Verifying the management server connection with the database – Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the default database • You change the IP address and host name of the computer that Symantec Endpoint Protection Manager runs on. See: Reconfiguring Symantec Endpoint Protection Manager after changing the computer's IP address and host name

More information

[Backing up the database and logs](#)

Reducing the database size when the database is full before an upgrade to Microsoft SQL Server Express

The default Microsoft SQL Server Express database has a size limit of 10 GB for data files and log data. When you upgrade from an embedded database with a size larger than 10 GB, and you are in the middle of the upgrade to Microsoft SQL Server Express, the upgrade process cannot continue.

If the Management Server Configuration Wizard detects that the database size is already too large, you may see the following messages:

The SQL Server Express database has reached its 10 GB limit. You must reconfigure the upgrade settings to import less data first. Then run the upgrade wizard again.

When the default database size is too large, pause the upgrade and perform the following steps:

Step 1: Decrease the number of days that logs are collected

In the following file, reduce the number of days: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties

- scm.sqlexpress.migration.otherlog.days=7
- scm.sqlexpress.migration.learnedapps.days=0
- scm.sqlexpress.migration.clientserveractivity.days=3
- scm.sqlexpress.migration.traffic.days=7
- scm.sqlexpress.migration.packet.days=7
- scm.sqlexpress.migration.security.days=7

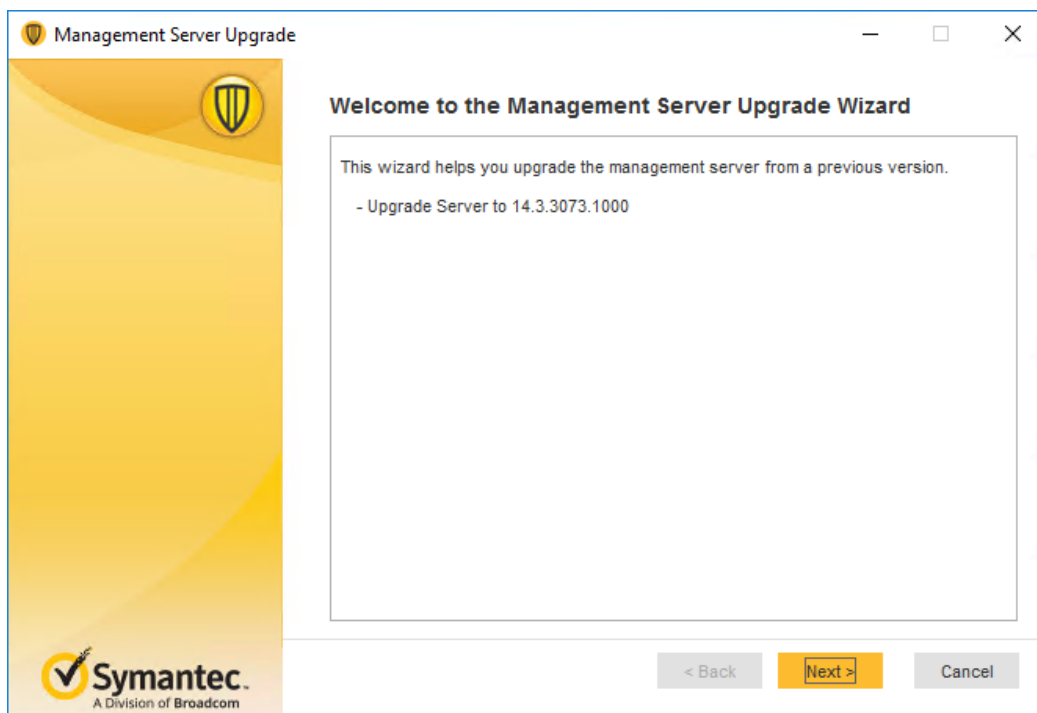
This reduces the amount of data that migrates to the SQL Server Express database.

NOTE

scm.sqlexpress.migration.clientserveractivity.days is already set to 7 by default to keep the database size smaller.

Step 2: Restart the Management Server Upgrade Wizard

Double-click ..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat



NOTE

If you had started the **Database Backup and Restore** dialog box before you made these changes, restart it by double-clicking `..\Symantec\Symantec Endpoint Protection Manager\bin\dbtools.bat`

More information

[Reducing the database size to less than 10 GB before an upgrade to Microsoft SQL Server Express](#)

Enabling FILESTREAM for the Microsoft SQL Server database

This topic describes how to enable FILESTREAM for a Microsoft SQL Server database.

The Microsoft SQL Server database uses a feature called FILESTREAM to reduce the database size and to improve database performance.

- The Microsoft SQL Server Express database has a 10 GB space limitation and requires FILESTREAM to be enabled. If you install your own SQL Server Express instance, you must enable FILESTREAM.
- If you upgrade from an embedded database (14.3 MP1 and earlier) to 14.3 RU1 and later, you do not need to enable the FILESTREAM; the upgrade wizard or configuration wizard enables FILESTREAM for you automatically.
- The Microsoft SQL Server database does not require FILESTREAM to be enabled, but it is recommended to improve performance. For a local SQL Server database, the Management Server Upgrade and Installation Wizard can enable FILESTREAM for you. For a remote Microsoft SQL Server database, you enable FILESTREAM manually on the computer where the SQL Server database is installed.

If you run the upgrade wizard or the configuration wizard and the following message appears, click **Yes**, and enable FILESTREAM.

The FILESTREAM feature is not enabled for this remote Microsoft SQL Server database.

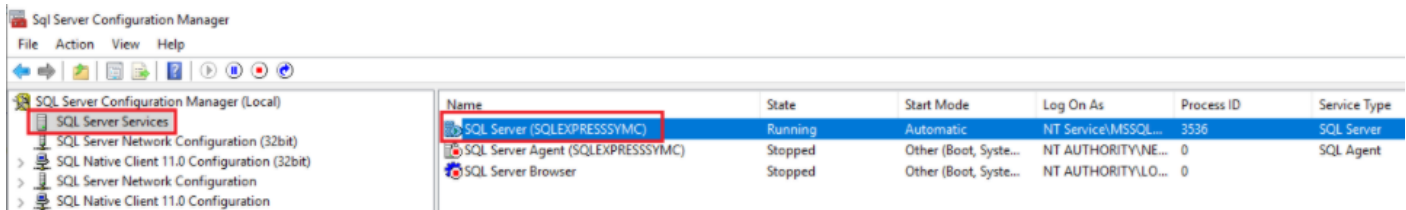
NOTE

Click **No** if you want to continue upgrading or installing and you do not want to enable the FILESTREAM feature at this time.

If you are upgrading, the Management Server Upgrade wizard closes. After you enable FILESTREAM, you must restart the upgrade wizard to continue the management server upgrade. On the Symantec Endpoint Protection Manager computer, click: `..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat`.

To enable FILESTREAM manually

1. On the **Start** menu, expand **Microsoft SQL Server** and then click **SQL Server Configuration Manager**.
2. In the **SQL Server Configuration Manager** list of services, select **SQL Server Services**, and then locate the instance of SQL Server on which you want to enable FILESTREAM.



3. Right-click the instance, and then click **Properties**.
4. In the **SQL Server Properties** dialog box, click the **FILESTREAM** tab.
5. Select the **Enable FILESTREAM for Transact-SQL access** and click **Enable FILESTREAM for file I/O streaming access** check boxes.
6. Click **Apply > OK**.
7. Restart the SQL Server database service by selecting the instance of SQL Server and clicking **Restart**.

More information

[FILESTREAM \(SQL Server\)](#)

Reducing the database size to less than 10 GB before an upgrade to Microsoft SQL Server Express

The default Microsoft SQL Server Express database has a size limit of 10 GB for data files and log data. Data files include items such as installation packages, virus definitions, policies, alerts, and learned applications. When you upgrade from the embedded database (14.3 MP1 and earlier) with a size larger than 10 GB, the upgrade process to SQL Server Express cannot continue. If the Management Server Configuration Wizard detects that the database size is too large, you may see the following message:

The backup exceeds the allowed SQL Server Express 10 GB limit. You must first reconfigure the management server to import less data. Then run the restore again.

The estimated data in the embedded database exceeds the Microsoft SQL Server Express limit of 10 GB. To continue the upgrade, the wizard must first reduce the amount of data to less than 10 GB.

You must first decrease the space in the existing embedded database, using one of the following tasks:

- Click **Continue** so that the Management Server Configuration Wizard decreases the database size at the beginning of the upgrade process.
- Cancel the Management Server Configuration Wizard, reduce the database size yourself, and restart the wizard using the following steps.

To reduce the amount of available database size manually

1. Remove any replication partners that Symantec Endpoint Protection Manager does not use.
For detailed information, see:
[Deleting sites](#)
2. Decrease the size of the logs and learned application data.
For detailed information, see:

Specifying the log size and how long to keep log entries in the database

Database Properties for SQLEXPRESS\$SYM

General Log Settings Backup Settings

Specify the size of logs maintained in the database for the site.

Management Server Log Settings

System Administrative Log Limit:	10000	entries	Expires after:	60	days
System Client-Server Activity Log Limit:	10000	entries	Expires after:	60	days
Audit Log Limit:	10000	entries	Expires after:	60	days
System Server Activity Log Limit:	10000	entries	Expires after:	60	days

Client Log Settings

Client Activity Log Limit:	10000	entries	Expires after:	60	days
Security Log Limit:	10000	entries	Expires after:	60	days
Traffic Log Limit:	50000	entries	Expires after:	60	days
Packet Log Limit:	10000	entries	Expires after:	60	days
Control Log Limit:	20000	entries	Expires after:	60	days

Risk Log Settings

Delete risk events after:	60	days	Compress risk events after:	7	days
Delete acknowledged notifications after:	30	days	Delete unacknowledged notifications after:	30	days
Delete scan events after:	30	days	Delete commands after:	30	days

☒ Delete unused virus definitions ☒ Delete EICAR events

OK Cancel Help

Site Properties for Local Site

General LiveUpdate Passwords Data Collection Private Insight Server

Site Settings

Site Name: Site

Description:

Console Timeout: 1 hour

☐ Keep track of every application that the clients run

☐ Delete learned application data after: 30 days

The management console uses the first server in the list to send reports and notification. If the server is not available, the management console uses the next server in the list. You can change the priority of servers by using the Move Up and Move Down buttons.

Move Up Move Down

3. Change the default settings for the database maintenance schedule.

- Stop the management server.
- In the following file: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties, decrease the number of seconds for the following entries.
scm.timer.objectsweep=1800
scm.timer.objectsweep.delay=60

NOTE

If these entries are not in the file, add them. This step increases the frequency that the database marks unwanted data as deleted.

For more information, see:

[Symantec Endpoint Protection Manager: How is Database Maintenance scheduled?](#)

- c. Restart the management server and wait for several hours or longer. See:
[Stopping and starting the management server service](#)
4. Schedule replication between all partners to occur at least once. Symantec recommends that you replicate more often.
For detailed information, see:
[Installing a new site as a replication partner to an existing site](#)
5. Wait for several hours after each scheduled replication before you restart the upgrade.
6. Rerun the database backup and then try to restore it.

Making more disk space available to upgrade to the default Microsoft SQL Server Express database

If the Symantec Endpoint Protection Manager (SEPM) computer does not have at least 10 GB of available disk space to upgrade to the Microsoft SQL Server Express database, you may see the following message:

```
The upgrade wizard cannot upgrade your embedded database to a Microsoft
SQL Server Express database. Either the destination drive does not
have enough available disk space, or the certificate is expired or will
expire within 10 days. Make sure there is at least x of free disk space
and that the certificate is current to continue.
```

You cannot continue the upgrade process, unless you make at least 10 GB of disk space available.

NOTE

SEPM blocks the upgrade if the certificate has either expired or is expiring in the next 10 days.

To increase disk space

1. Remove unused files and temporary files.
The Windows temporary files are at:
 - C:\Windows\Temp
 - C:\Users\<username>\AppData\Local\TempFor more information, see:
[Disk cleanup in Windows 10](#)
2. Empty the Recycle Bin.
3. If the previous steps do not reduce enough disk space, remove more SEPM files.
 - a. Stop the management server service using the Run command: `net stop semsrv`
For more information, see:
[Stopping and starting the management server service](#)
 - b. Move the following SEPM files to another disk drive:
 - ..\Symantec\Symantec Endpoint Protection Manager\Inetpub\ClientPackages
 - ..\Symantec\Symantec Endpoint Protection Manager\Inetpub\content
 - ..\Symantec\Symantec Endpoint Protection Manager\data\backup
 - ..\Symantec\Symantec Endpoint Protection Manager\data\inbox
 - c. Restart the management server service.
4. Change database backup settings.
 - Make sure the **Number of database backups to keep** option is set to 1, the default.
 - Keep **Back up logs** unchecked.For more information, see:
[Running automatic database backups](#)

-
5. Move files that the Symantec Endpoint Protection Manager does not use to another disk drive.

If the certificate has expired, see:

[Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server](#)

Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server

Symantec Endpoint Protection Manager uses a certificate to authenticate communications between the Symantec Endpoint Protection (SEPM) and the Microsoft SQL Server Express or SQL Server databases. You must generate the certificate and import it into the Symantec Endpoint Protection Manager computer for SEPM to connect to either SQL Server database. If the certificate does not exist, is expired, or is about to expire, the connection between SEPM and the database fails.

You can install or upgrade the management server and either SQL Server database if you have not imported the certificate. However, the Management Server Configuration Wizard detects whether the certificate is already expired or expires within the next 30 days. SEPM sends a notification every day until the 30 days is over to remind the administrator to import the certificate. You may see the following message:

Within the next 30 days, Symantec Endpoint Protection Manager will no longer be able to connect to the Microsoft SQL Server database because SQL Server uses a certificate that is about to expire.

NOTE

You only need to update the SEPM certificate using the following steps when the SEPM and the SQL server share the same expiring certificate.

Step 1: Generate a self-signed certificate

If your organization does not already have a Certificate Authority (CA) signed certificate, you must generate one. This step describes how to generate and replace the default self-signed Symantec Endpoint Protection Manager (SEPM) certificate with a CA-signed certificate. See:

[Use a signed certificate with Endpoint Protection Manager](#)

Step 2: Configure a permanent certificate for SQL Server

You must enable encrypted connections for an instance of the SQL Server Database Engine and must use SQL Server Configuration Manager to specify the certificate. See the "Configure server" section at:

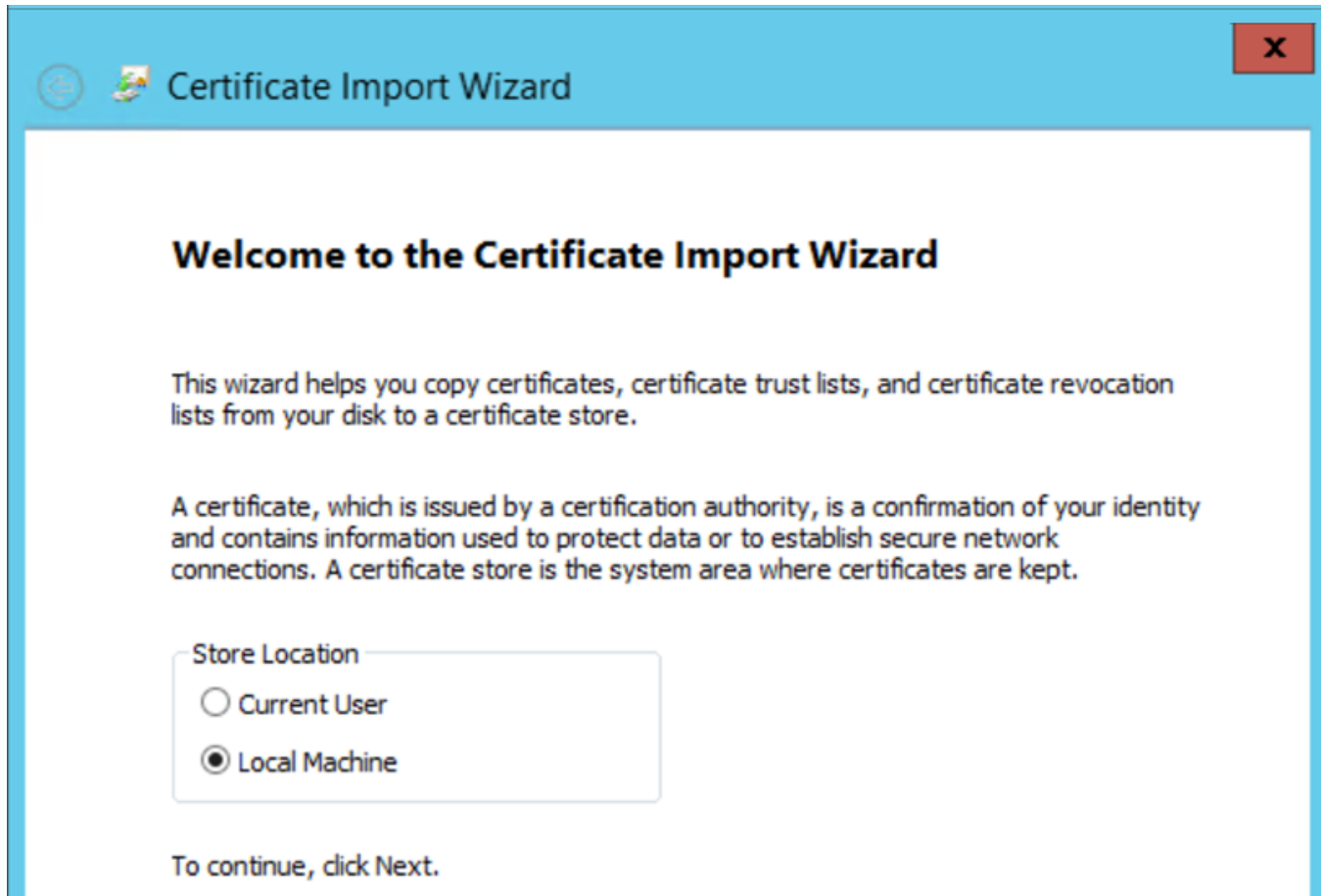
[Enable encrypted connections to the Database Engine](#)

Step 3: Import the SQL Server certificate into Windows on the Symantec Endpoint Protection Manager computer

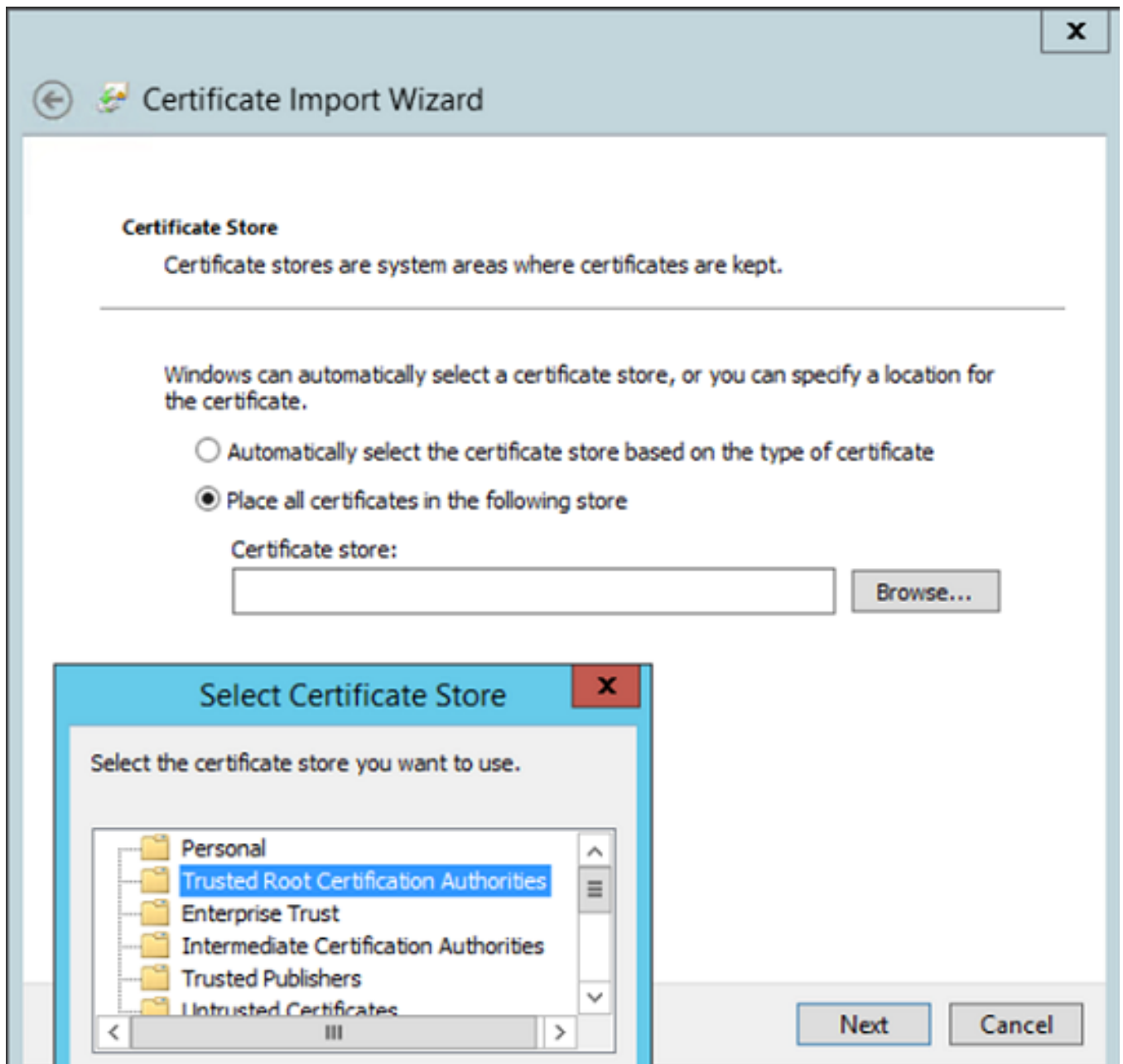
The management server computer must have the SQL Server public certificate provisioned. To provision the certificate on the management server computer, you import it into Windows. The management server computer must be set up to trust the certificate's root authority.

To import the SQL Server certificate into Windows on the Symantec Endpoint Protection Manager computer

1. On the management server computer, select **Run** from the **Start** menu, and then type `certmgr.msc`.
2. In the Certificate Manager, select Trusted Root Certificate Authorities and click All Tasks > Import.
These steps may vary, depending on the Windows Server version.
3. In the Welcome to the Certificate Import Wizard, right-click the certificate, and then click **Install Certificate**.
4. In the Certificate Import Wizard, follow the steps to import the certificate.
 - Click **Local Machine**, and then click **Next**.



- Click **Place all certificates in the following store**, click **Browse**, and in the Select Certificate Store dialog box, click **Trusted Root Certification Authorities**.



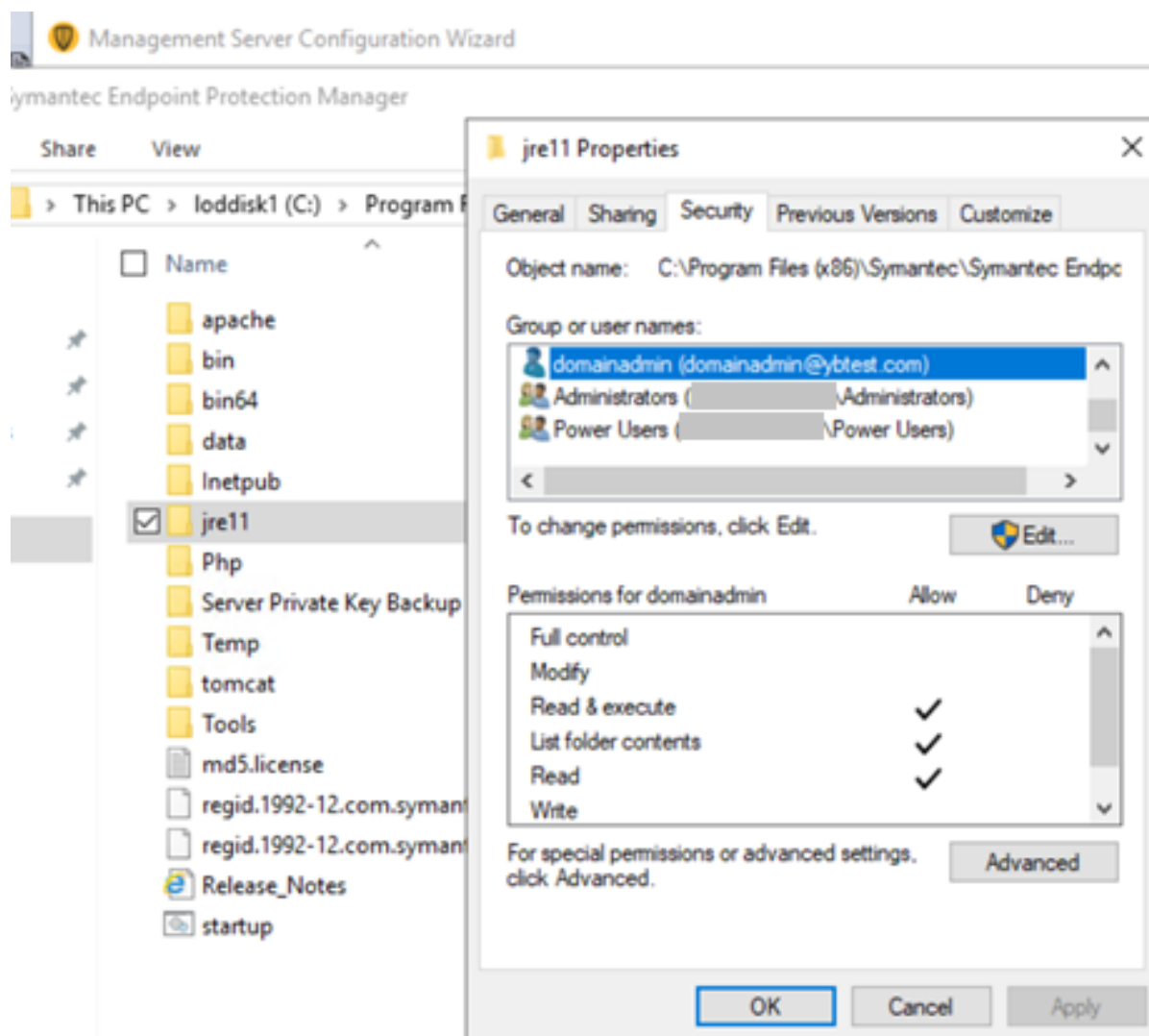
5. Click **OK**, and then click **Next**.

Step 4: Configure permissions for the jre11 folder

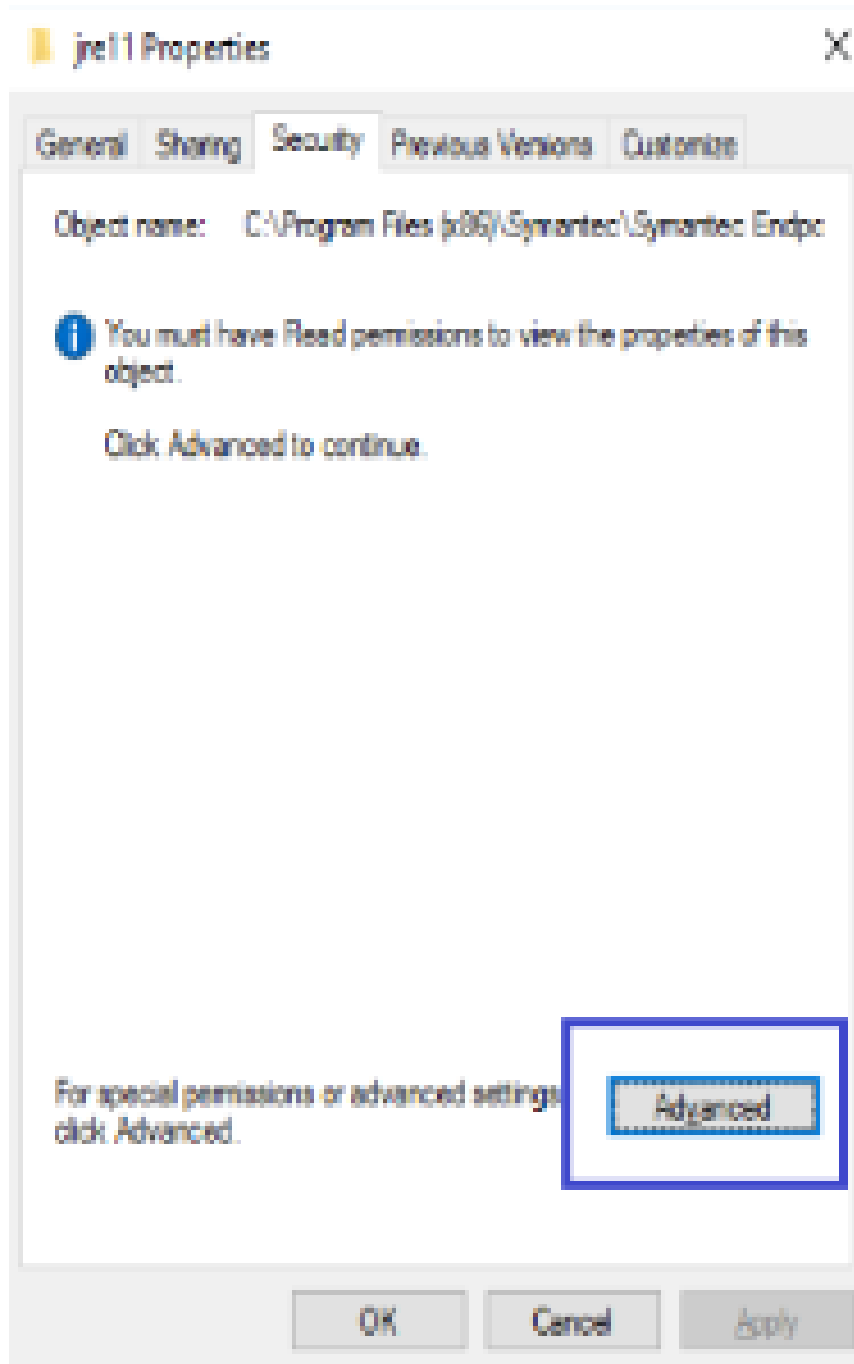
NOTE

If your SQL Server is configured using a domain admin with Windows authentication, the domain admin needs to have **Read & execute**, **List folder contents**, and **Read** permissions for the jre11 folder on the Symantec Endpoint Protection Manager server.

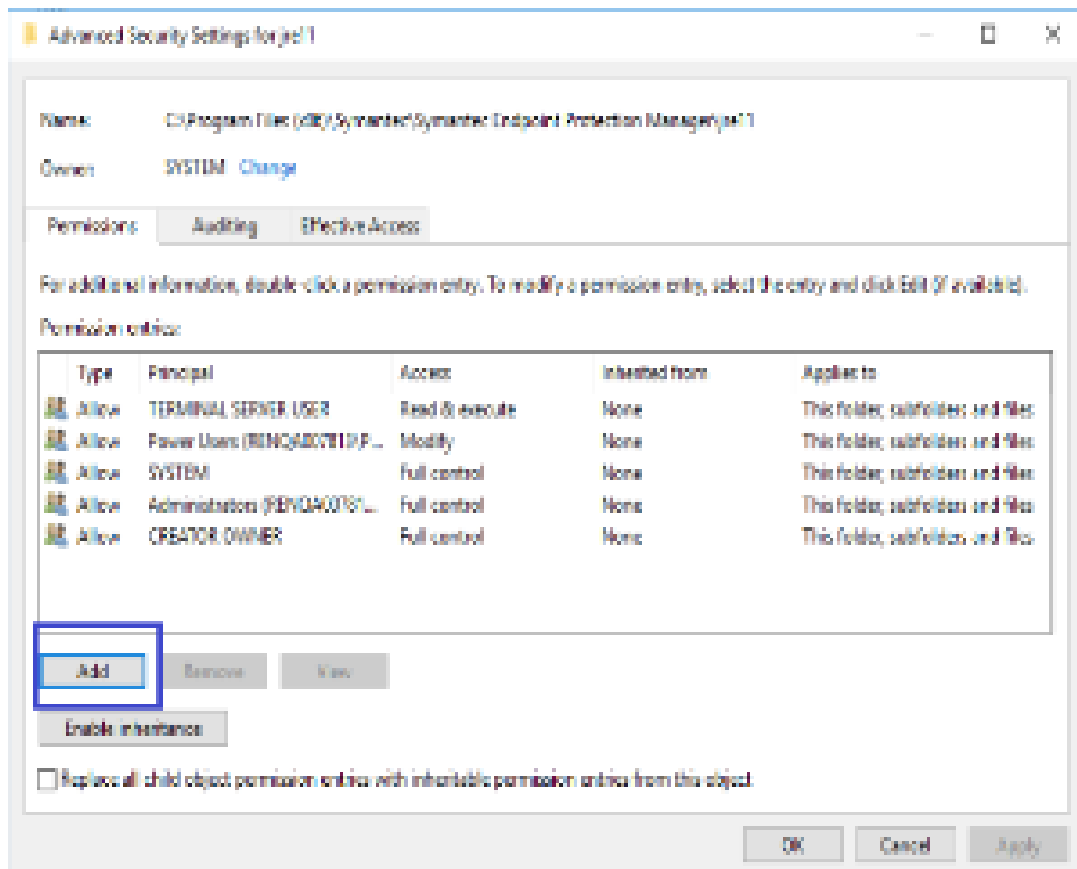
1. On the Symantec Endpoint Protection Manager server, go to `\...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager` folder, right-click the jre11 folder, and click **Properties**.



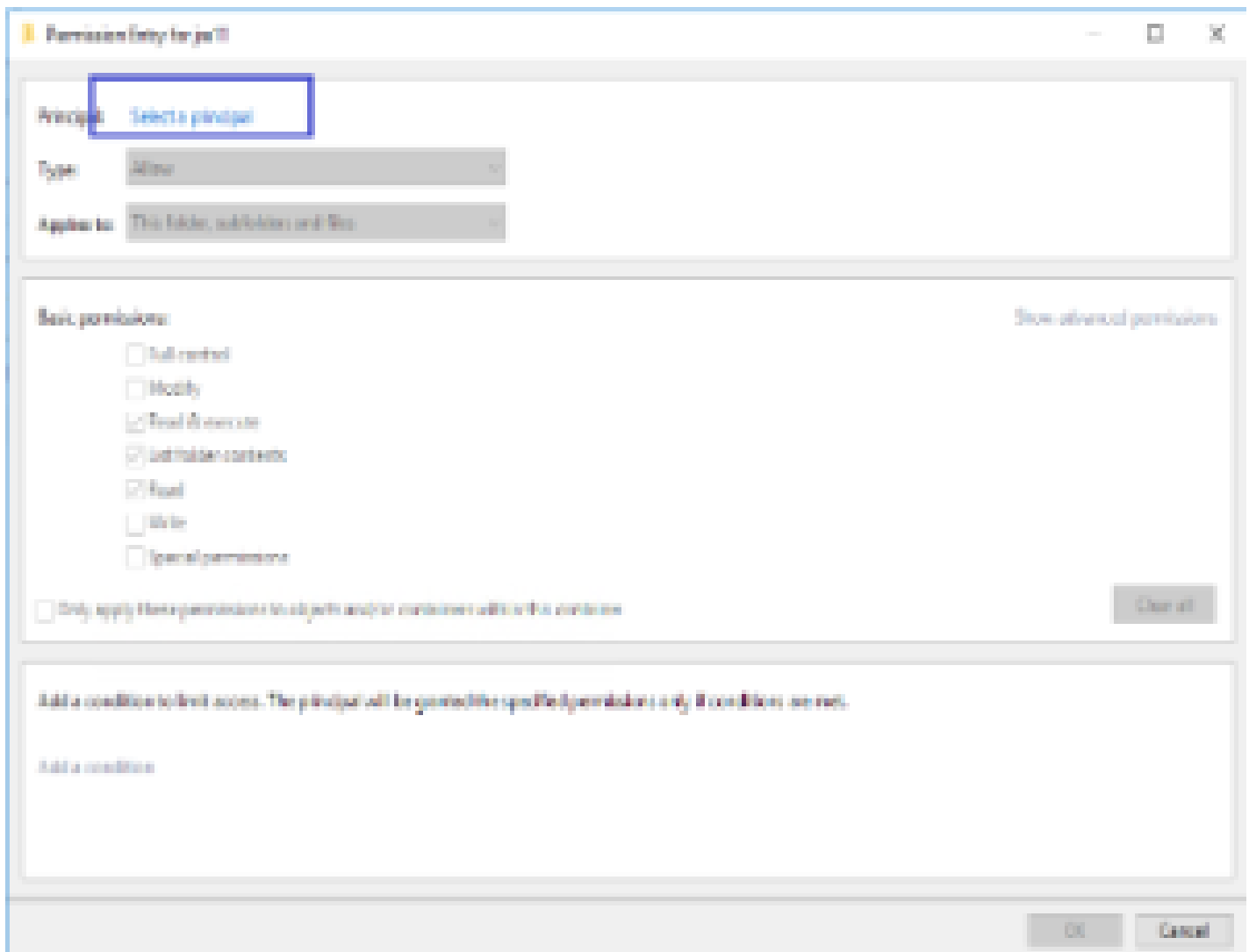
2. In the file properties window, on the **Security** tab, click **Advanced**.



3. In the **Advanced Security Settings** window, on the **Permissions** tab, click **Add**.



4. In the **Permissions Entry** window, click **Select a principal**.



5. In the **Select User, Computer, Service Account, or Group** window, add the **domainadmin** user, and click **OK**.

Select User, Computer, Service Account, or Group

Select this object type:

User, Group, or Built-in security principal

Object Types...

From this location:

sep.com

Locations...

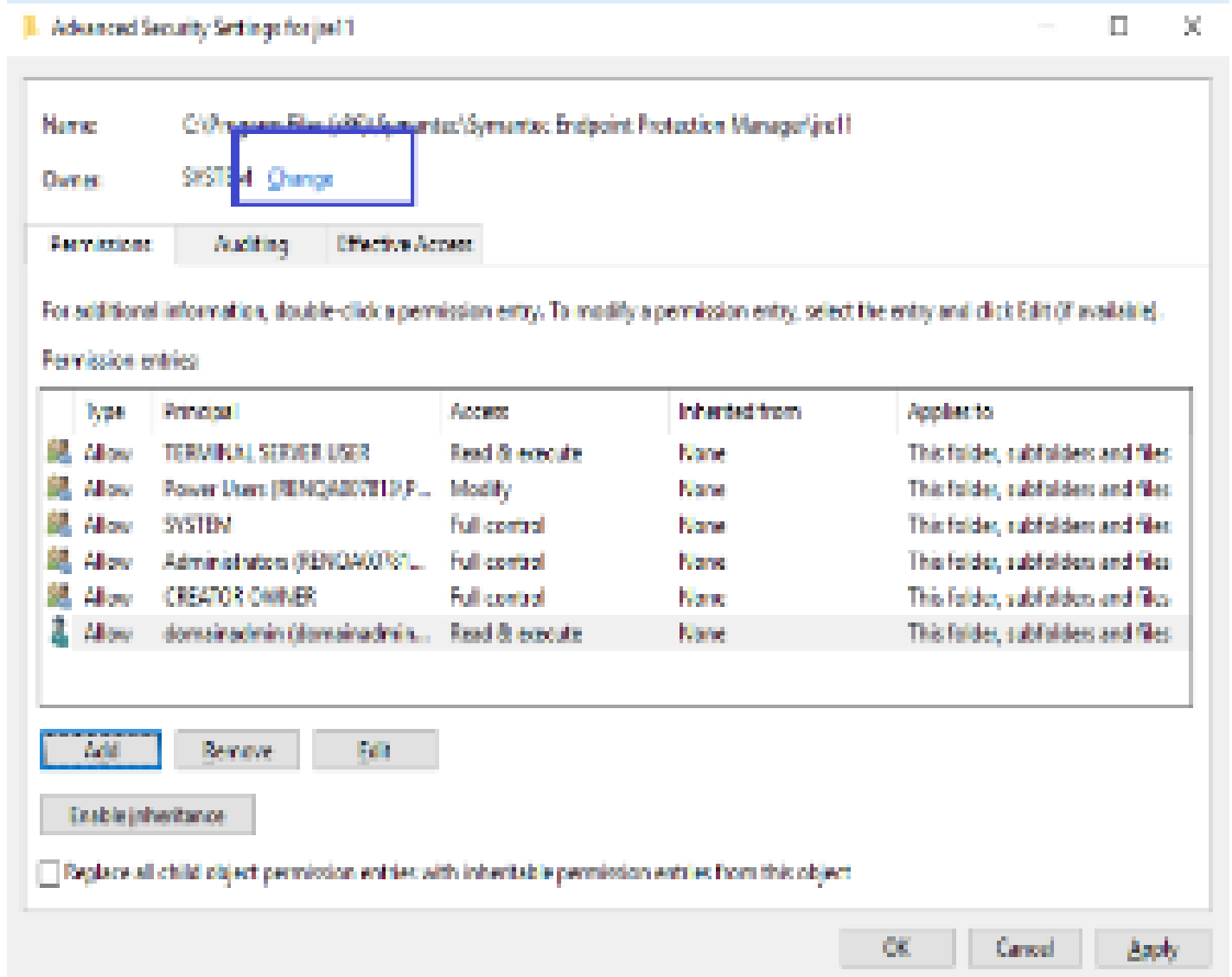
Enter the object name to select (examples):

domainadmin (domainadmin@sep.com)

Check Names

Advanced... OK Cancel

6. In the **Permissions Entry** window, click **OK**.
7. In the **Advanced Security Settings** window, on the **Permissions** tab, select **domainadmin**, and click **Change**.



8. In the **Select User, Computer, Service Account, or Group** window, add the **domainadmin** user again, and click **OK**.

Select User, Computer, Service Account, or Group

Select this object type:

User, Group, or Built-in security principal

Object Types...

From this location:

sep.com

Locations...

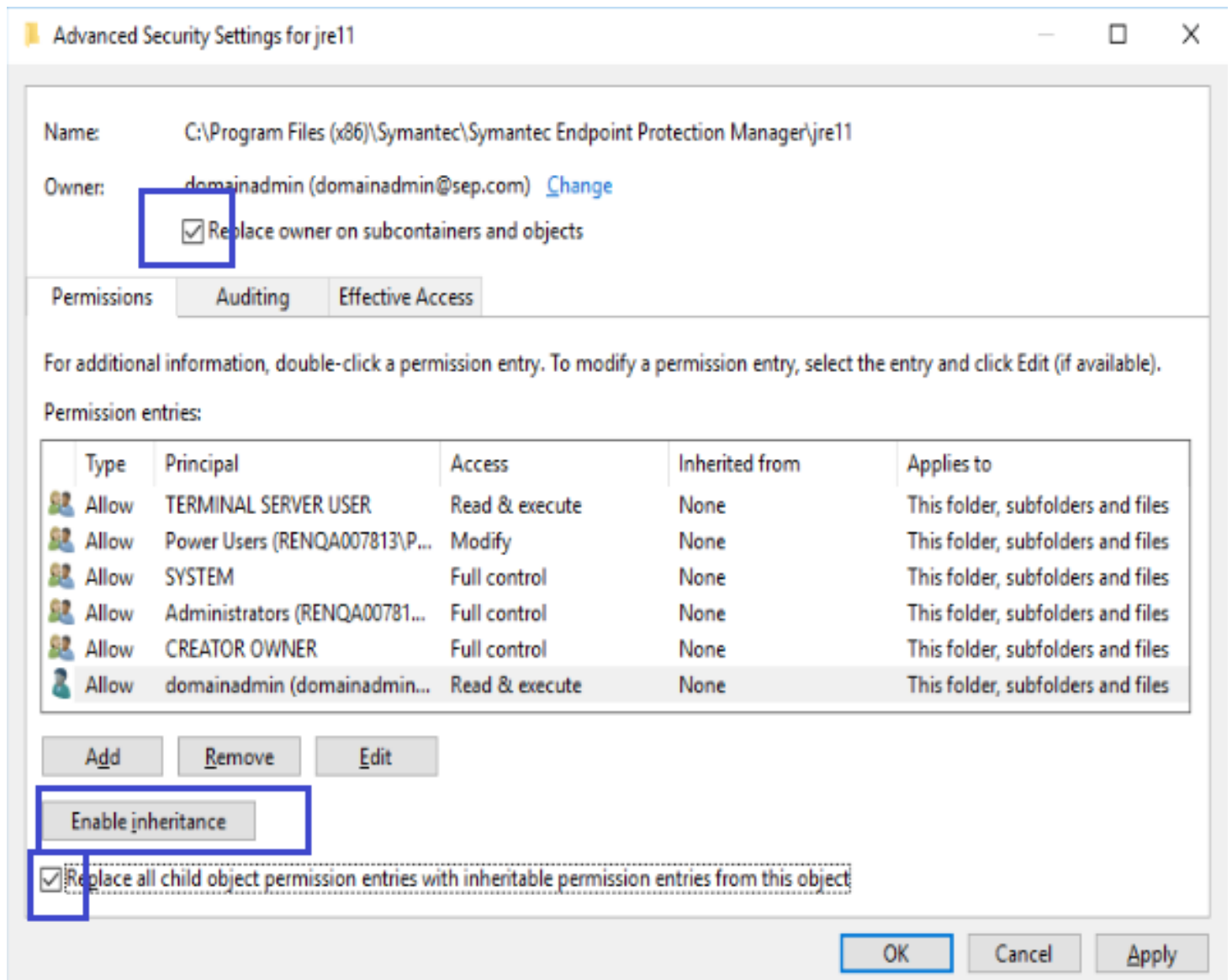
Enter the object name to select (examples):

domainadmin (domainadmin@sep.com)

Check Names

Advanced... OK Cancel

9. In the **Advanced Security Settings** window, check **Replace owner on subcontainers and objects**, check **Replace all child object permission entries with inheritable permission entries from this object**, click **Enable inheritance**, and click **Apply**.



10. Click **Yes** and **OK** to confirm.

11. In the file properties window, make sure that the **domainadmin** user has now all required permissions, and click **OK**.

Step 5: Open the Management Server Configuration Wizard and complete the Server Configuration with Windows Authentication option

- To open the wizard, go to \...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin folder, and double-click sca.bat file.

Management Server Configuration Wizard

Step One: Database Server Authentication
This step must be completed first.

Authentication type: Windows Authentication

Database server: WIN-database.com

SQL server port: 1433

Windows user name: sep/domainadmin

Windows user password: *****

SQL Server client folder: C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\1130\Tools\Binn\ Browse... (required)

Connect to database

Step Two: New Database Creation

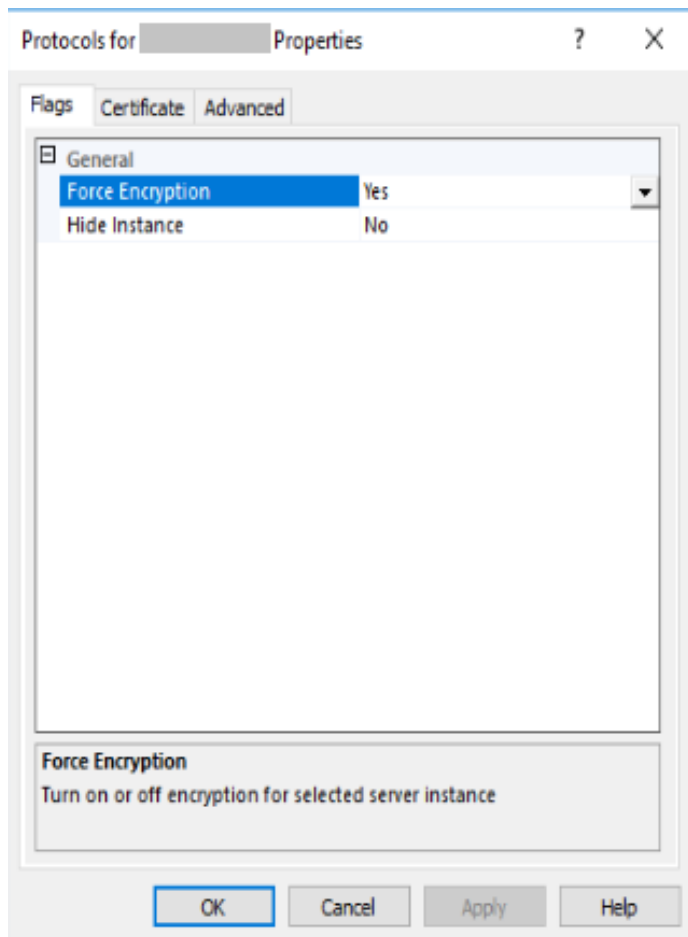
Database name: sem5

Database data folder: C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQLDATA\

< Back Next > Cancel

Step 6: Check if the communication is encrypted and using the SQL Server certificate

1. On the management server, open the following file: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\conf\Catalina\localhost\root.xml and make sure that **encrypt=true** and **trustServerCertificate=false**.
2. On the SQL Server, open **Protocols for MSSQLSERVER Properties**, and check if **Force Encryption=Yes**.



3. On the SQL Server, run the following query, to check if the connection between Symantec Endpoint Protection Manager and SQL Server is encrypted:

```
SELECT session_id, connect_time, net_transport, encrypt_option, auth_scheme, client_net_address FROM sys.dm_exec_connections
```

Check if **encrypt_option=TRUE**.

SQLQuery1.sql - RE...Administrator (53)) * X

```
SELECT session_id, net_transport, encrypt_option, auth_scheme, client_net_address FROM sys.dm_exec_connections
```

100 %

Results Messages

	session_id	net_transport	encrypt_option	auth_scheme	client_net_address
1	51	Shared memory	TRUE	NTLM	<local machine>
2	52	TCP	TRUE	SQL	
3	53	Shared memory	TRUE	NTLM	<local machine>
4	54	Shared memory	TRUE	NTLM	<local machine>
5	55	TCP	TRUE	SQL	
6	58	TCP	TRUE	SQL	
7	57	TCP	TRUE	SQL	
8	59	TCP	TRUE	SQL	
9	60	TCP	TRUE	SQL	

Symantec Endpoint Protection Manager has detected that the configured email server or directory server requires certificate verification to be disabled

Symantec Endpoint Protection Manager (SEPM), you may see one of the following messages on the last screen of the Management Server Upgrade wizard:

- Symantec Endpoint Protection Manager has detected that the configured email server requires certificate verification to be disabled, which can disclose sensitive data to unauthorized third parties. You should review your email server certificate and configuration so that certificate verification can be enabled.
This message may appear if you upgrade from 14.3 RU3 or earlier to 14.3 RU4 or later.
- Symantec Endpoint Protection Manager has detected that the configured directory server(s) require certificate verification to be disabled, which can disclose sensitive data to unauthorized third parties. You should review your directory server certificate and configuration so that certificate verification can be enabled.
This message may appear if you upgrade from 14.3 RU5 or earlier to 14.3 RU6 or later.

These messages occur if the Symantec Endpoint Protection Manager had previously disabled certificate verification to communicate with the email or directory server. During the upgrade, the Symantec Endpoint Protection Manager then detects that your configured email server certificate or directory server certificate cannot be verified. However, Symantec recommends that you enable the verification of the server certificate so that the connection to the email server or directory server is more secure.

Step 1: (Optional) Create a personal CA root certificate for Active Directory

If you do not already have a personal CA root certificate for Active Directory, perform the following steps to create one.

If the following steps do not match what you see, check with the vendor, such as Microsoft.

To create and export the server certificate

- Log on as a domain administrator on the Active Directory domain server.

-
2. Click **Start > Control Panel > Administrative Tools > Certificate Authority** to open the CA Microsoft Management Console (MMC).
 3. Right-click the CA computer, and select **CA Properties**.
 4. On the **General** menu, click **View Certificate**.
 5. Select the **Details** view and click **Copy to File** in the lower-right corner of the window.
 6. Use the Certificate Export wizard to save the CA certificate in a file.

Step 2: Install the server certificate into Windows on the Symantec Endpoint Protection Manager computer

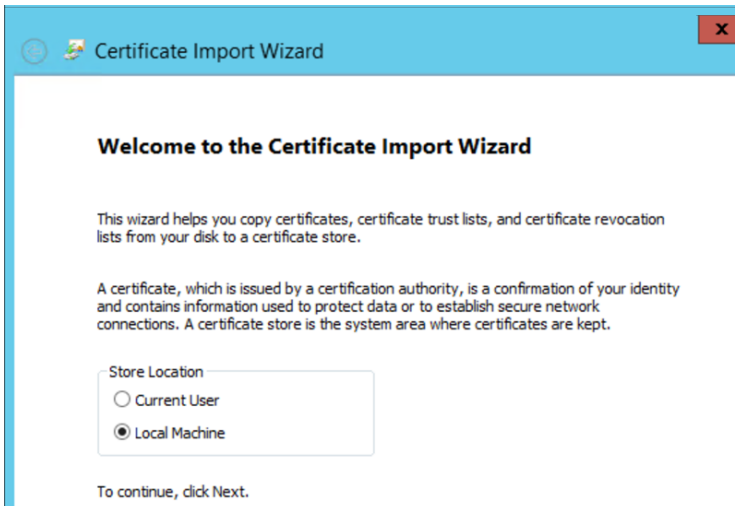
You then import the email server or directory server certificates, which use the DER, PEM, or PFX extension.

To import the server certificate into Windows on the management server computer

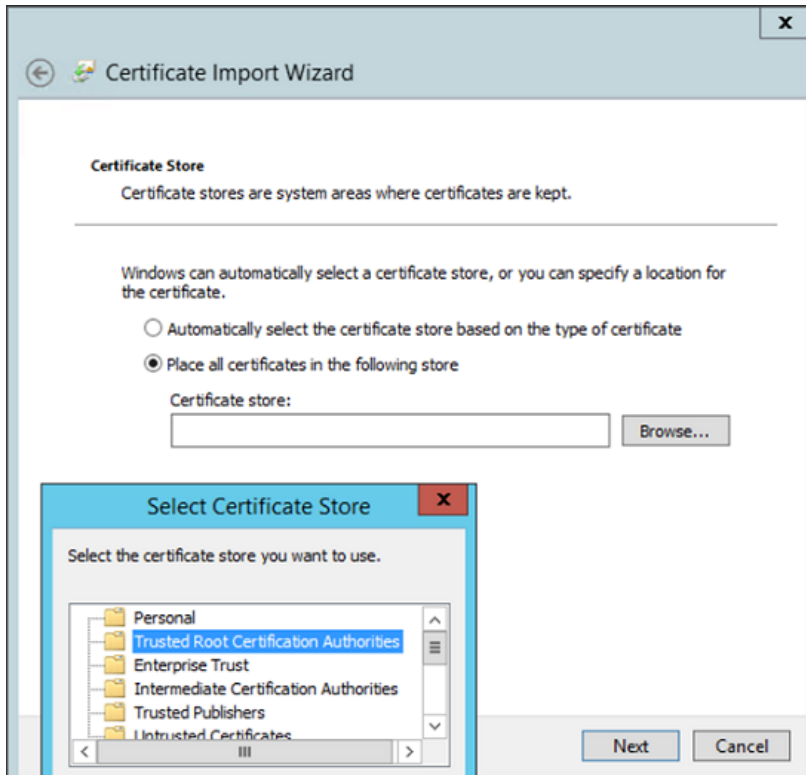
1. Export the server certificate to the Windows computer where Symantec Endpoint Protection Manager is installed.
2. Right-click the certificate and click **Install Certificate**.



3. In the **Certificate Import Wizard** dialog box, under **Store Location**, select **Local Machine**, and then click **Next**.



4. Select **Place all certificates in the following store**, click **Browse**, and in the **Select Certificate Store** dialog box, click **Trusted Root Certification Authorities**.



5. Click **OK**, and then click **Next**.

Step 3: Enable server certificate verification

You must enable certificate validation so that SEPM can connect to the email server or directory server. After you enable certificate validation, SEPM checks that the certificate is valid.

To enable email server certificate verification

1. On the console, stop and restart the management server service using the following commands:

```
net stop semsrv, net stop semapisrv, net start semsrv, net start semapisrv
```

[Stopping and starting the management server service](#)

2. Click **Admin > Servers**, right-click the management server, and click **Edit the server properties**.
See: [Establishing communication between the management server and email servers](#)
3. On the **Email Server** tab, uncheck the **Disable verification of the email server certificate** option and then click **OK**.

To enable directory server certificate verification

1. On the console, stop and restart the management server service using the following commands:

```
net stop semsrv, net stop semapisrv, net start semsrv, net start semapisrv
```

2. Click **Admin > Servers**, right-click the management server, and click **Edit the server properties**.
3. On the **Directory Servers** tab, select the server and then click **Edit**.
4. Uncheck the **Disable verification of the email server certificate** option and then click **OK**.
If a warning appears that the validation or the Symantec Endpoint Protection Manager cannot connect to the directory server, check the certificate and validate it again until the warning disappears.

NOTE

If the administrator is configured to use Directory Server authentication, repetitively clicking the warning may impact the Symantec Endpoint Protection Manager administrator login and it may lock out the administrator.

[Unlocking an administrator account after too many logon attempts](#)

[Choosing the authentication method for administrator accounts](#)

For information on adding a directory server, see:

[Connecting to a directory server on a replicated site](#)

Resolving Microsoft SQL Server database connection errors after 14.3 RU5 or later installation or upgrade

You may need to change the DB Owner Account permissions or recreate the reporting database account to address errors that occur when you install or upgrade to Symantec Endpoint Protection Manager (SEPM) 14.3 RU5 or later.

You may see the following error after installation or upgrade:

```
The Symantec Endpoint Protection Manager reporting account does not connect to the
Microsoft SQL Server database. You must recreate or modify the reporting account in
SQL Server Management Studio. Then run the Management Server Configuration Wizard again.
```

This error most likely occurs because the current DB Owner Account does not have the `[ALTER ANY LOGIN]` permission, but may also occur for the following reasons:

- You may have a password mismatch. The Reporting Account uses the same password as the DB Owner Account. If you reset the password of the DB Owner Account, you must reset the Reporting Account to use the same password. For a new installation, the SEPM Management Server Configuration Wizard creates a SEPM database with the DB Owner Account and the Reporting Account. For example, if the database name is `sem5` and the DB Owner Account is `sem5`, the Reporting Account is `REPORTER_sem5sem5` (formatted as "REPORTER_<DatabaseName><DBOwnerAccount>").
- The Reporting Account login and User are corrupted or don't match each other.

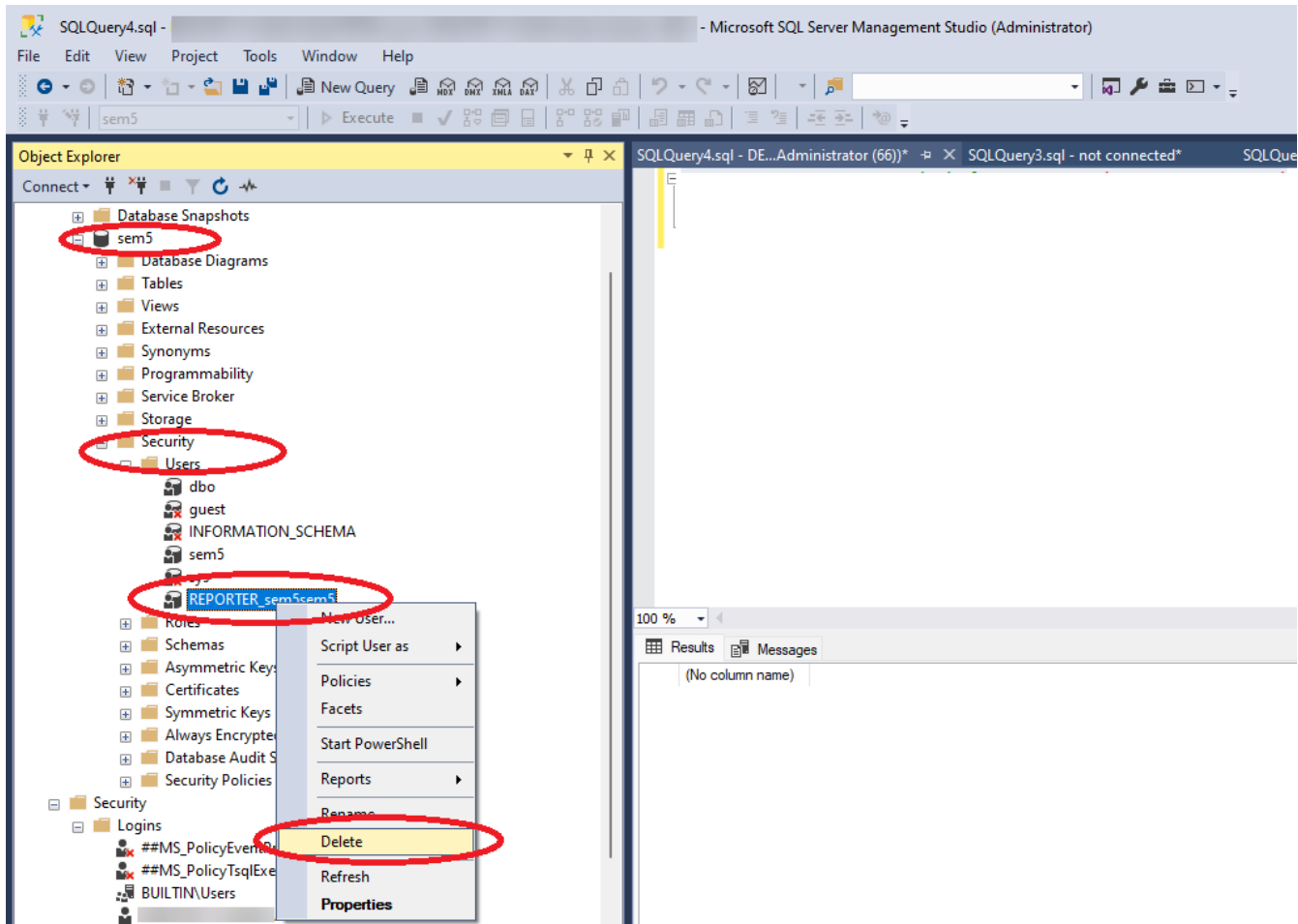
Solutions

To resolve this error, try either of these solutions:

- Grant `[ALTER ANY LOGIN]` permission to the DB Owner Account and then reconfigure or rerun the upgrade by double-clicking `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat` to finish running the Management Server Configuration Wizard.
- If you do not want to grant this permission to the DB Owner Account, you can recreate the reporting database account on Microsoft SQL Server Management Studio.

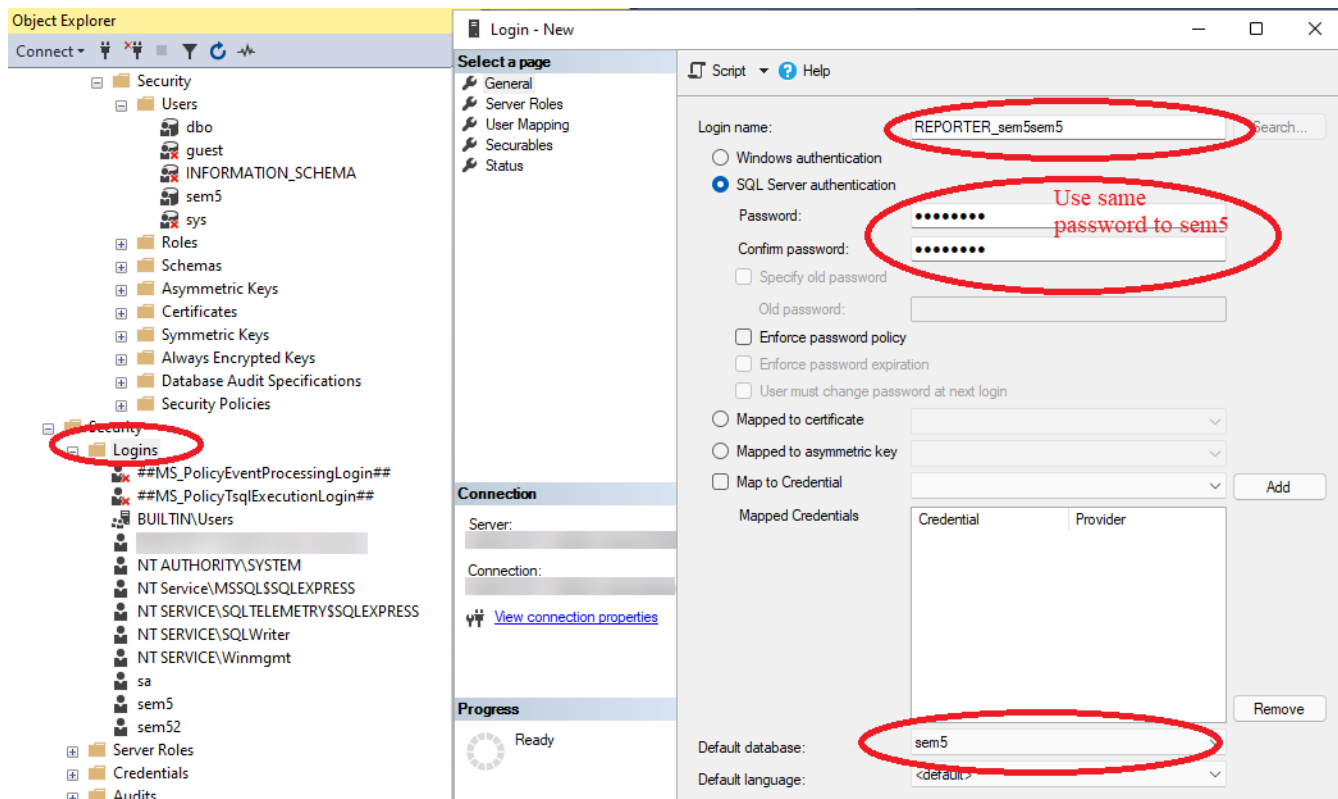
To recreate the reporting database account on Microsoft SQL Server Management Studio

1. On the Microsoft SQL Server computer, open Microsoft SQL Server Management Studio.
2. Delete the Reporting Account user account, if it exists.
 - a. In the Object Explorer, select the Symantec Endpoint Protection Manager database (**sem5** by default).
 - b. Expand **Security > Users**, and then right-click **REPORTER_<DatabaseName><DBOwnerAccount>**.
 - c. Click **Delete**.

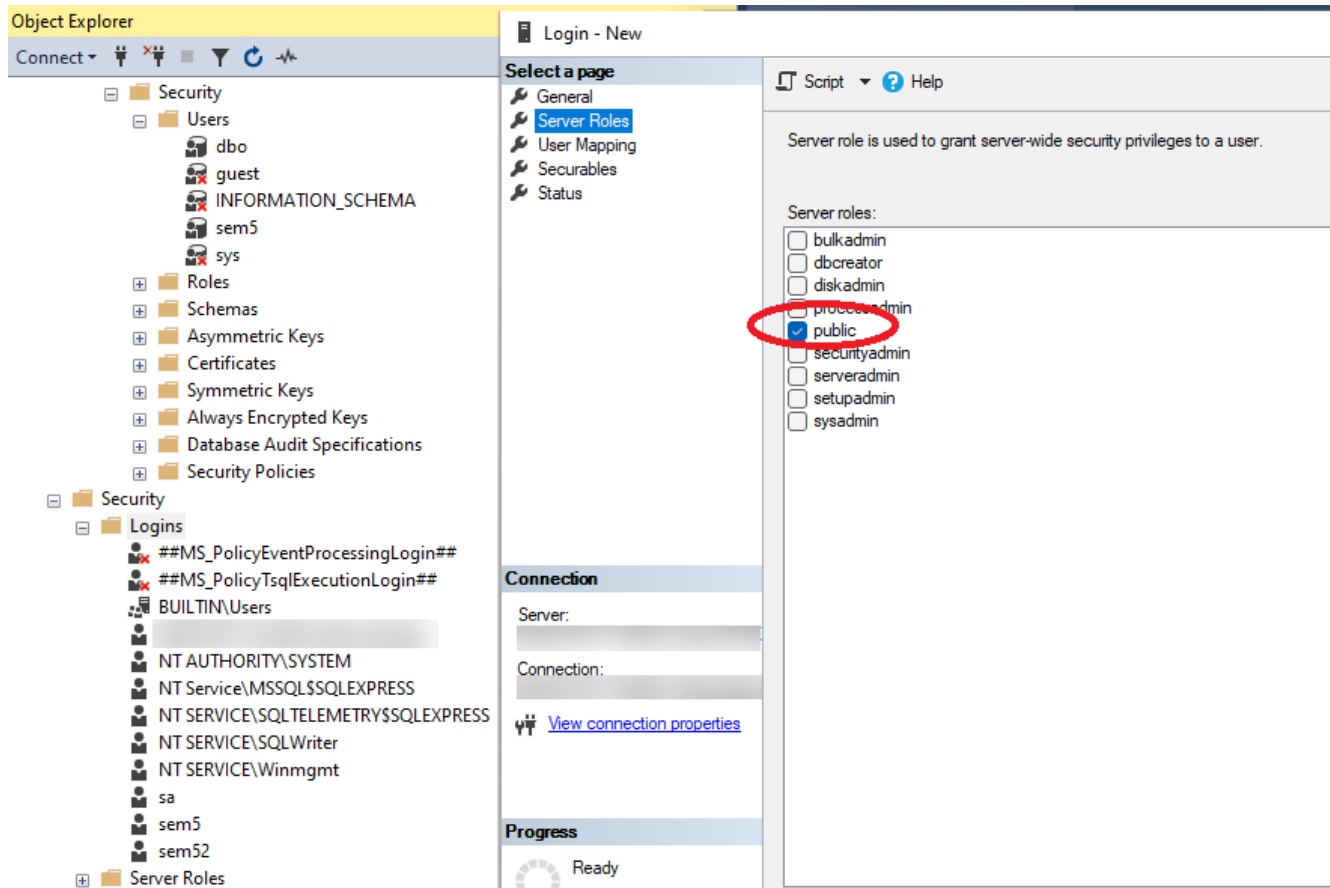


3. Modify or recreate the login for the Reporting Account.

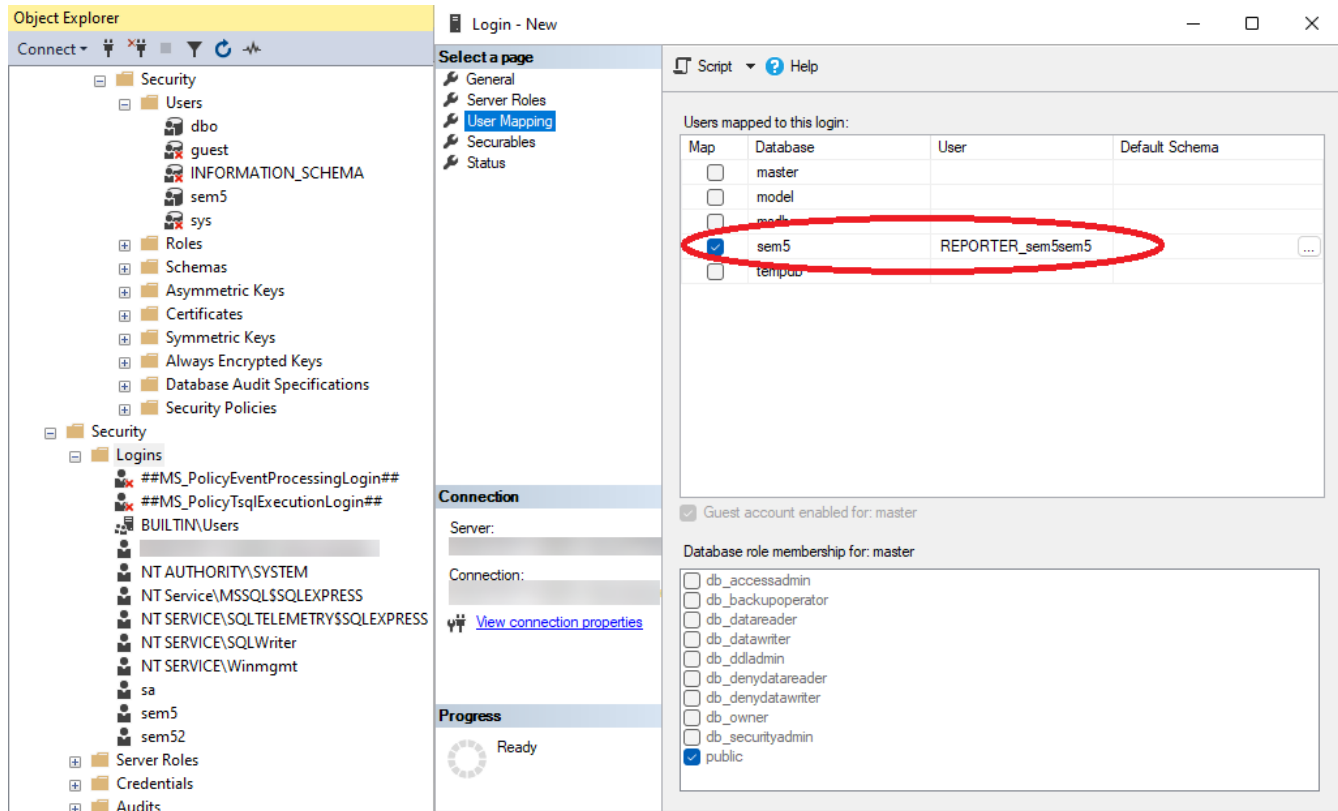
- Expand **Security > Logins**, and then select your database.
- On the **Login > General** page, select your **Login name**.
- Under **SQL Server authentication**, type the password for your DB Owner Account.
If your DB Owner Account uses Windows Authentication, type and confirm your Windows account password.
- Select the **Default database** as your database.



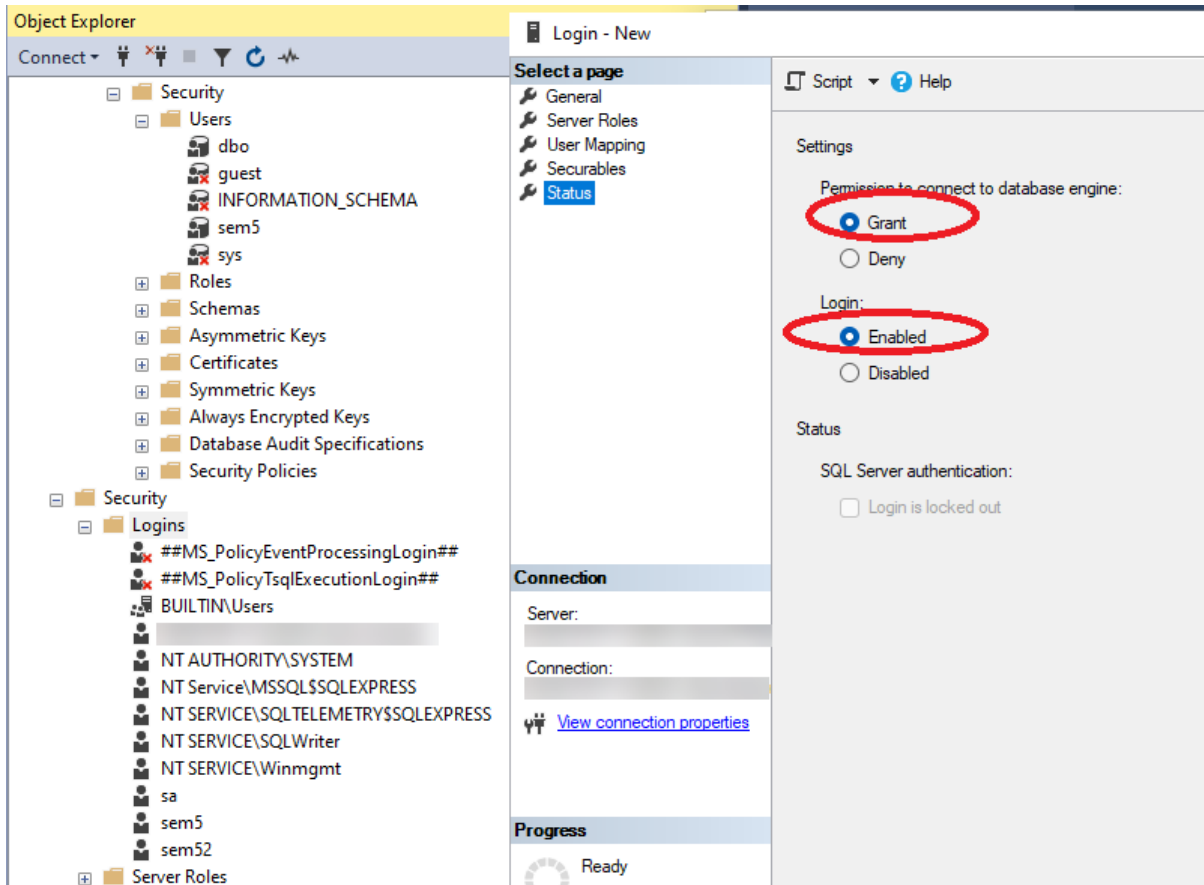
4. On the **Server Roles** page, select the **public** server role.



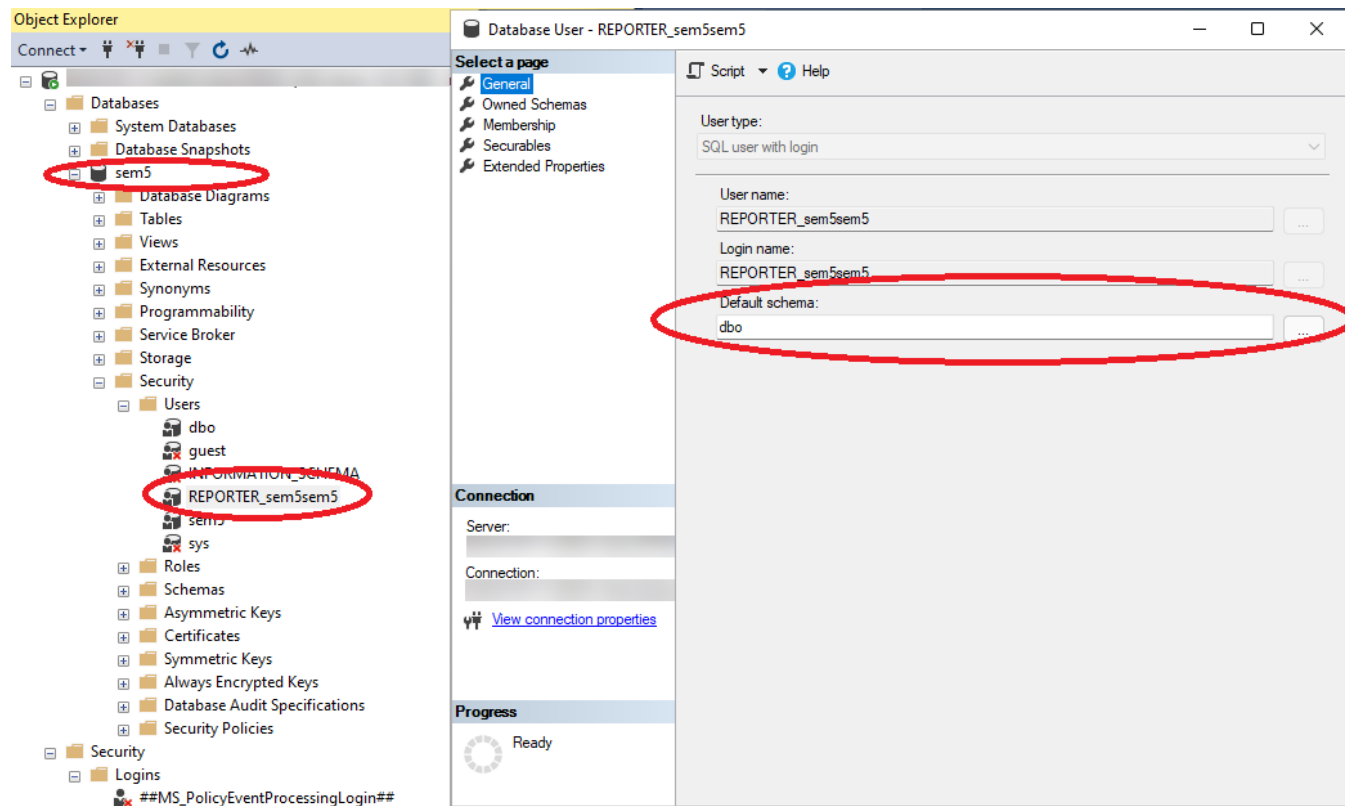
5. On the **User Mapping** page, map the login account to your database.



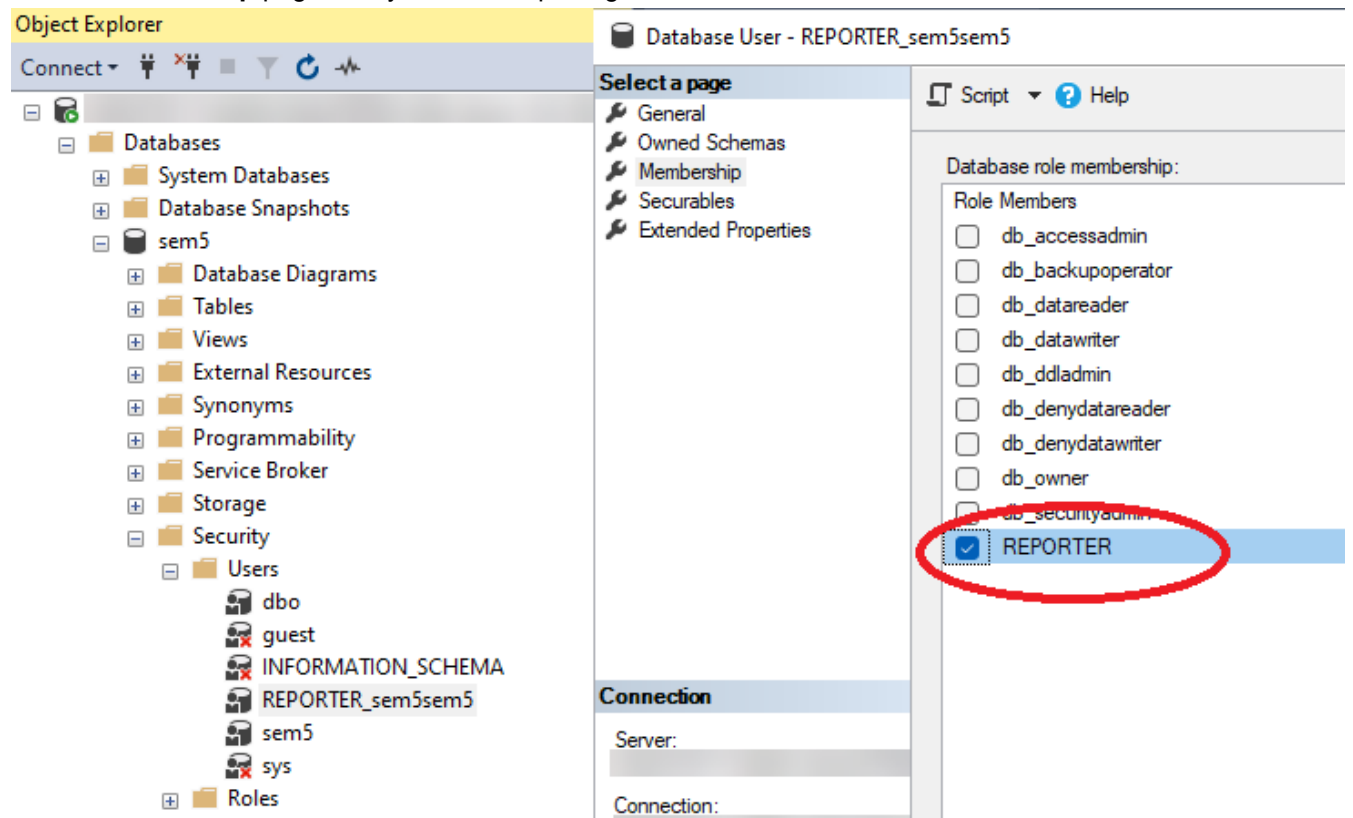
6. On the **Status** page, do the following:
 - a. Set the permission to **Grant**.
 - b. Set the login account to **Enabled**.
 - c. Click **OK**.



7. Reconfigure or rerun the upgrade. Double-click `upgrade.bat` to finish rerunning the Management Server Configuration Wizard.
8. (Optional) After you finish, you can verify your changes. Do the following:
 - a. On the **General** tab, verify that the Reporting Account user uses the correct Default schema.



- b. On the **Membership** page, verify that the Reporting Account user has the role **REPORTER**.



The console should now correctly show the homepage.

Upgrading an environment that uses multiple embedded databases and management servers

An environment that uses multiple embedded database and management servers has the following implications:

- The management servers do not use failover or load balancing for Symantec Endpoint Protection because the embedded database does not support failover or load balanced servers.
- The management servers are Symantec Endpoint Protection replication partners.

All sites have a computer on which you first installed the management server. You must upgrade this management server first, because it contains critical site information such as the encryption key or encryption password. You then upgrade the other management servers that you installed for replication.

NOTE

As of 14.3 RU1, the Microsoft SQL Server Express database replaces the embedded database. SQL Server Express supports failover and load balancing.

To upgrade an environment that uses multiple embedded databases and management servers

1. Authenticate to and log on to the computer on which you installed the first Symantec Endpoint Protection Manager.
Do not log on to Symantec Endpoint Protection Manager. If you use replication, you do not need to disable it first. Symantec Endpoint Protection does not allow replication if the product versions do not match.
2. Upgrade the management server.
3. Upgrade all additional management servers one by one.

Reconfiguring Symantec Endpoint Protection Manager after changing the computer's IP address and host name

The Symantec Endpoint Protection clients use the host name and IP address of the Symantec Endpoint Protection Manager (SEPM) computer to communicate with SEPM. If you change the computer's host name and the IP address, the clients do not automatically maintain communication. Furthermore, the SEPM cannot connect to the database because the database server's name has changed and its previous certificate with the old computer name and IP address is not valid.

The SEPM web console displays a certificate error because the IP address and host name of the SEPM computer are different from what is in the certificate. See:

[Troubleshooting: Your server certificate is not valid because the computer host name or IP address changed \(14.3 RU8 or later\)](#)

NOTE

You perform these tasks when SEPM and the SEP clients communicate over HTTPS only, and not HTTP.

Reconfiguring the Symantec Endpoint Protection Manager and generating a certificate for the SQL Server Express or SQL Server databases

To reconfigure Symantec Endpoint Protection Manager and generate a certificate for the SQL Server Express or SQL Server databases

1. In the Symantec Endpoint Protection Manager, update the management server list to use both the current and the new host name and IP address, and make sure it is assigned to all clients.

The updated list allows SEP client to continue to communicate with SEPM after host name and IP address changes.
See:

[Assigning a management server list to a group and location](#)

2. On the **Clients > Policies** tab, click the **General > Security Settings** tab, and clear **Enable secure communications between the management server and clients by using digital certificates for authentication**.
Disabling secure communications allows the clients to still communicate with the SEPM without needing to authenticate communications with the SEPM. See:
[Updating the server certificate on the management server without breaking communications with the client](#)
3. On the **Clients > Clients** tab, verify that the clients are still connected to the management server.
4. Change the SEPM computer IP address.
5. Change the SEPM computer host name, and then restart the SEPM computer.

NOTE

You can rename just the computer host name and not necessarily the IP address.

6. Stop the SEPM services by running the following commands: `net stop semsrv`, `net stop semapisrv`, and `net stop semwebsrv`. See:

[Stopping and starting the management server service](#)

7. Open the following files:

`<SEPM_Install>\tomcat\conf\Catalina\localhost\root.xml`

`<SEPM_Install>\tomcat\instances\sepm-api\conf\Catalina_WS\localhost\jdbc.properties`

where `<SEPM_Install>` is the Symantec Endpoint Protection Manager installation directory

- a. Change:

`jdbc:sqlserver://<sepm_old_computer_name>:2638`

To:

`jdbc:sqlserver://<sepm_new_computer_name>:2638`

NOTE

If you use a different port number than 2638, continue to use the other number.

- b. Change:

`trustServerCertificate = false`

To:

`trustServerCertificate = true`

8. In the registry location `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MSSQLServer\Client\ConnectTo`, change:

Value name: `<old_sql_express_db_instance>\<sql_express_instance_name>`

Value data: `DBMSSOCN,<old_server name>\<sql_express_instance_name>,2638`

To:

Value name: `<new_sql_express_db_instance>\<sql_express_instance_name>`

Value data: `DBMSSOCN,<new_server name>\<sql_express_instance_name>,2638`

For example:

Value name: `WIN-newserver\SQLEXPRESSSYMCO`

Value data: `DBMSSOCN,WIN-newserver.xxx.labs.abc.net\SQLEXPRESSSYMCO,2638`

9. Restart the Symantec Endpoint Protection Manager service by running the following commands: `net start semsrv`, `net start semapisrv`, and `net start semwebsrv`.
10. Log on to Symantec Endpoint Protection Manager.
 - If the Your server certificate is not validated. message appears, update the certificate, and then log on (14.3 RU8 or later).

For information about solving this issue, see: [Troubleshooting: Your server certificate is not valid because the computer host name or IP address changed \(14.3 RU8 or later\)](#)

- If the `Failed to connect to the server` message appears, click **OK** and log on anyway (14.3 RU7 or earlier).

11. Generate a new SEPM server certificate.

This step matches the SEPM-to-SEP client certificate information with the new computer name and IP address. See: [Generating a new server certificate](#)

12. Log off from the SEPM console.

13. Do one of the following steps:

Microsoft SQL Server Express database	1. Reconfigure SEPM. See: Reinstalling or reconfiguring Symantec Endpoint Protection Manager 2. Log on to SEPM.
Microsoft SQL Server database	1. Reconfigure SEPM. The TLS message appears. 2. Generate and import a new SQL TLS certificate. Complete the configuration. 3. Log on to SEPM. If the SQL Server database is on the same computer as SEPM, see: Reconnecting the Microsoft SQL Server database to the clients after changing the computer's host name
Embedded database	Log on to SEPM.

14. Click **Enable secure communications between the management server and clients by using digital certificates for authentication**.

15. Verify that the clients are still connected to SEPM.

Reconnecting the Microsoft SQL Server database to the clients after changing the computer's host name

If you use the Microsoft SQL Server as the database server on the same computer as SEPM, the server name that is used for ODBC connections changes after you change the computer host name. You must update the server name that is used for ODBC connections. You can only change the computer name of SEPM and not the IP address.

To change the server name that ODBC connections uses

1. On the Symantec Endpoint Protection Manager computer, click **Start > Run**.
2. In the Name field, type either `odbc32.cpl` (32-bit) or `odbcad32.exe` (64-bit) and click **OK**.
3. In the **ODBC Data Source Administrator** dialog box, click the **System DSN** tab.
4. Click **SymantecEndpointSecurityDSN** as the System DSN and click **Configure**.
5. Enter the correct connection destination for the server name, such as the back slash (\), and then click **Next**.
6. If you use Windows authentication, select **With Integrated Windows authentication**. If you use SQL Server authentication, select **With SQL Server authentication using a login ID and password entered** and then input your Login ID and password. Click **Connect to SQL Server to obtain default settings for the additional configuration options**, and then click **Next**.
7. Select **Change the default database to**, select **sem5**, and then click **Next**.
8. Click **Finish**.
9. On the ODBC Microsoft SQL Server dialog box, click **Test Data Source**.
If you see the message `TEST COMPLETED SUCCESSFULLY!`, the ODBC connection test is finished.

Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate (14.3 RU9 or later)

Starting in 14.3 RU9, the Symantec Endpoint Protection Manager installation and upgrade requires that the management server name must also match one of the Subject Alternate Names (SANs) listed in the server certificate. In addition, the server name must use a valid host name, fully qualified domain name (FQDN), or IP address.

If the management server name and the SAN do not match, do one of the following steps to continue.

- Rename the management server.
- Update the certificate because the management server name is correct but the server certificate is not. See: [Updating or restoring a server certificate](#)

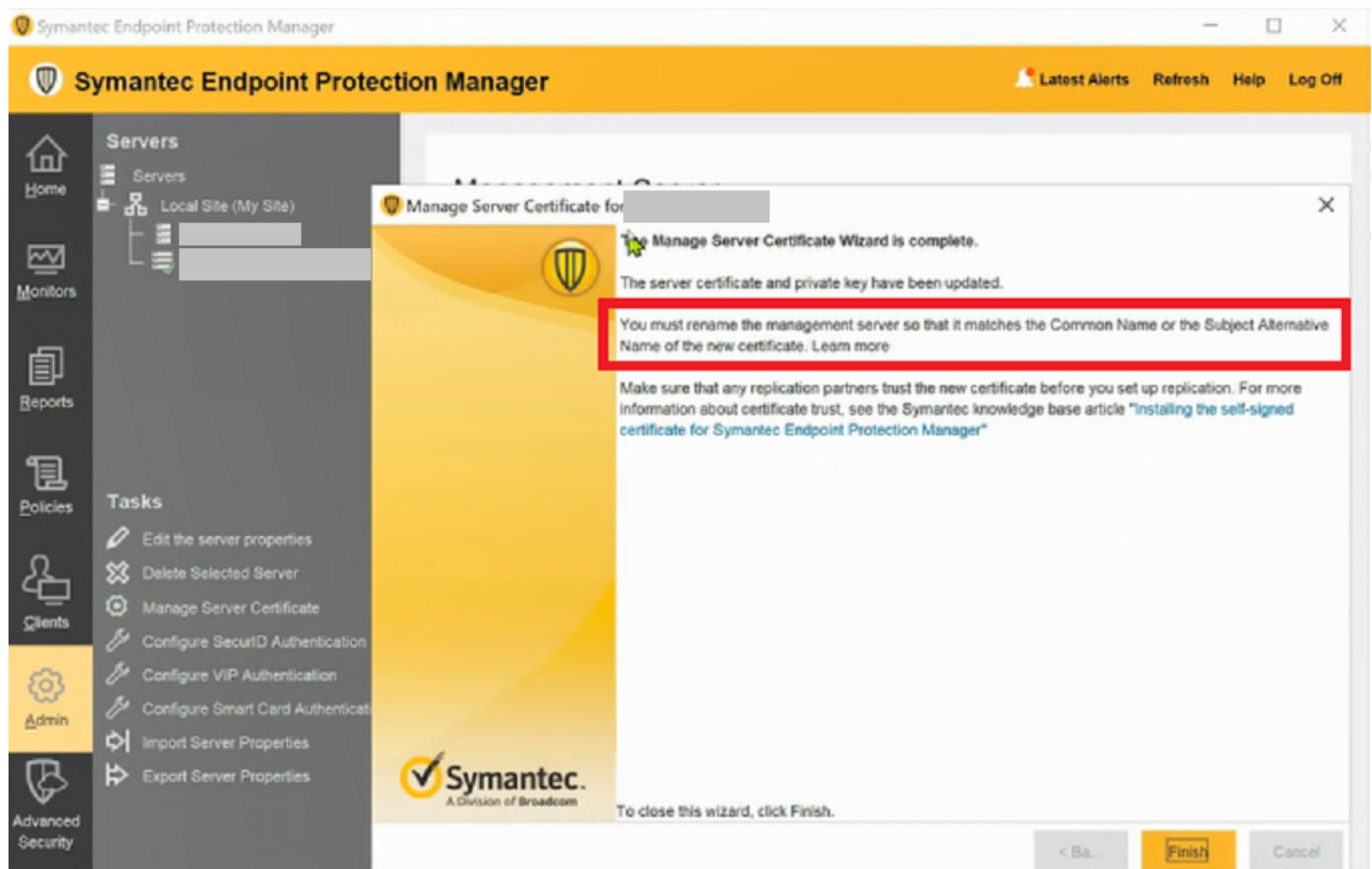
Condition

This issue occurs in the following situations:

Scenario 1:

You import a new certificate with one or more SANs that do not match the current management server name. After you import the certificate, you see the following message in the **Manage Server Certificate** wizard:

You must rename the management server so that it matches the Common Name or the Subject Alternative Name of the new certificate.



Scenario 2:

You may see the following message:

- The secure connection to Symantec Endpoint Protection Manager that uses the current server name cannot be established. You must resolve one or more of the following issues before you can continue the upgrade:
 - If the server name is an invalid hostname, fully qualified domain name, or IP address, or if it does not match one of the Subject Alternate Name(s) (SAN) listed in the server certificate, you must rename the server or update your server certificate.
 - If the server certificate is self-signed, check that the Symantec Endpoint Protection Manager computer trusts the certificate.

This message appears in the following cases:

- You import a new server certificate from a 14.3 RU8 and earlier SEPM but did not rename the management server to match the server name in the imported certificate.
- You rename the management server from what is in the certificate and then start the upgrade.

Cause

This issue occurs for either of the following reasons:

- The management server name is not a DNS name that resolves to the Symantec Endpoint Protection Manager computer IP address.
- The DNS name is not part of the management server certificate SAN list.

In both cases, the current management server name does not meet the new requirement in 14.3 RU9.

Solution

Make the server names match in both the certificate and the management server by changing the server name in the Management Server Configuration Wizard.

NOTE

If you do not perform this task, you cannot upgrade to 14.3 RU9 or later.

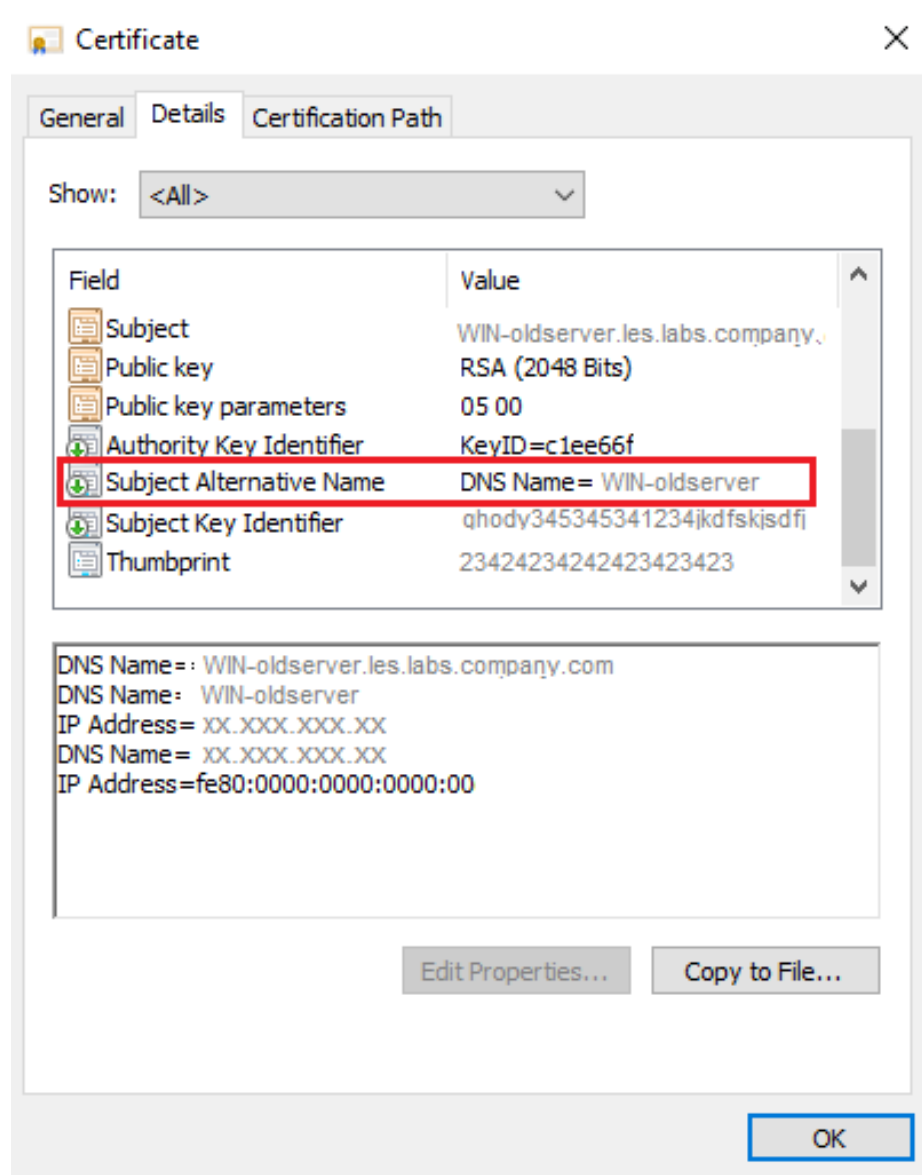
To reconfigure the management server name to match the SAN in the server certificate

1. Click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Management Server Configuration Wizard**.
2. Clear the **Use a recovery file to restore communication with previously deployed clients** option, and then click **Next**.

The recovery file includes the original certificate file before you imported a new one. If you do not clear this option, you would overwrite the certificate that you imported.
3. In the **Specify the site name** panel, change the **Server name** to the same one that is in the imported server certificate.

To find the server name in the certificate, do the following steps:

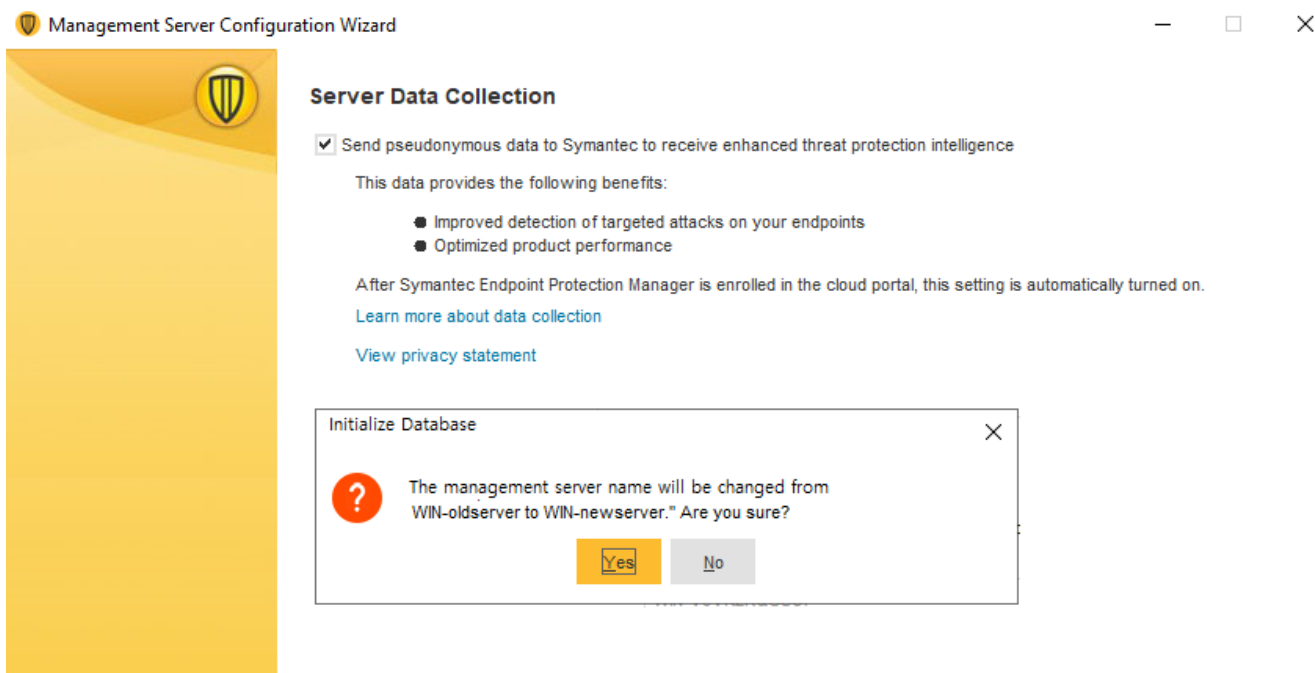
 1. Double-click the <SEPM_Install>\apache\conf\ssl\server.crt file.
 2. On the **Certificate** dialog box > **Details** tab, copy the values in the **Subject Alternative Name** or the **IP Address** field.



4. Click **Next**.

5. Keep the remaining default values in each panel.

If you correctly changed the server name, on the **Server Data Collection** panel, the following message appears:



Click **Yes**.

6. After the wizard finishes updating the database, try upgrading again.

If you completed the steps correctly, you should not see the message that blocks the upgrade.

If you cannot log on, the management server name still does not match what is in the certificate.

Other issues

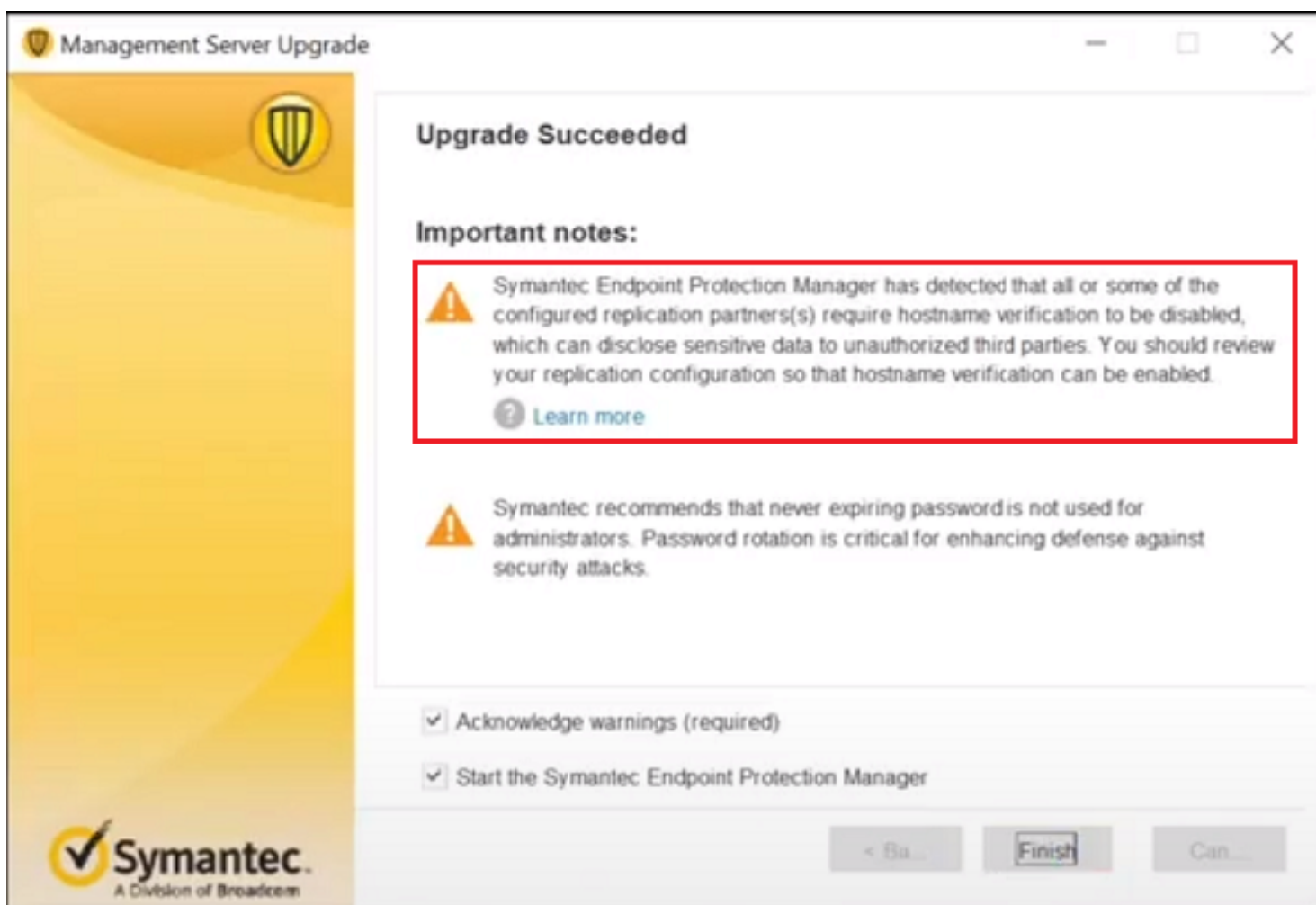
If you use a self-signed certificate rather than a publically signed certificate, make sure that SEPM computer trusts the certificate. See:

[Accepting the self-signed server certificate for Symantec Endpoint Protection Manager](#)

Symantec Endpoint Protection Manager detected that the configured replication partner requires host name verification to be disabled (14.3 RU9 or later)

After you upgrade to Symantec Endpoint Protection Manager (SEPM) 14.3 RU9 or later, you may see the following message on the last screen of the Management Server Upgrade wizard.

Symantec Endpoint Protection Manager has detected that all or some of the configured replication partner(s) require hostname verification to be disabled, which can disclose sensitive data to unauthorized third parties. You should review your replication configuration so that hostname verification can be enabled.



This message appears in the following situations:

- You upgraded from 14.3 RU8 or earlier to 14.3 RU9 or later.
- The replication partner host name or IP address that is specified by the local management server does not match one or more Subject Alternative Names (SANs) in the partner management server certificate.

During the upgrade, the Symantec Endpoint Protection Manager detects that your configured replication partner certificate host name cannot be verified. Therefore, to keep the connection with the replication partner, SEPM disables verification.

However, you should reenable the verification of the replication partner server host name so that the connection to the replication partner is more secure.

Reenable verification and update the partner server host name

To reenale verification, do the following tasks:

- Reenable the requirement that the management server verifies the replication partner server host name.
- Make sure that the replication partner servers and the local management server use the same host name. You change the replication partner host name in the Replication Server Management Server List. Edit the list so that the host names or IP addresses match the certificate of the respective replication partner server.

To reenale verification and update the partner server host name

1. Click **Admin > Servers > Replication Partners**.

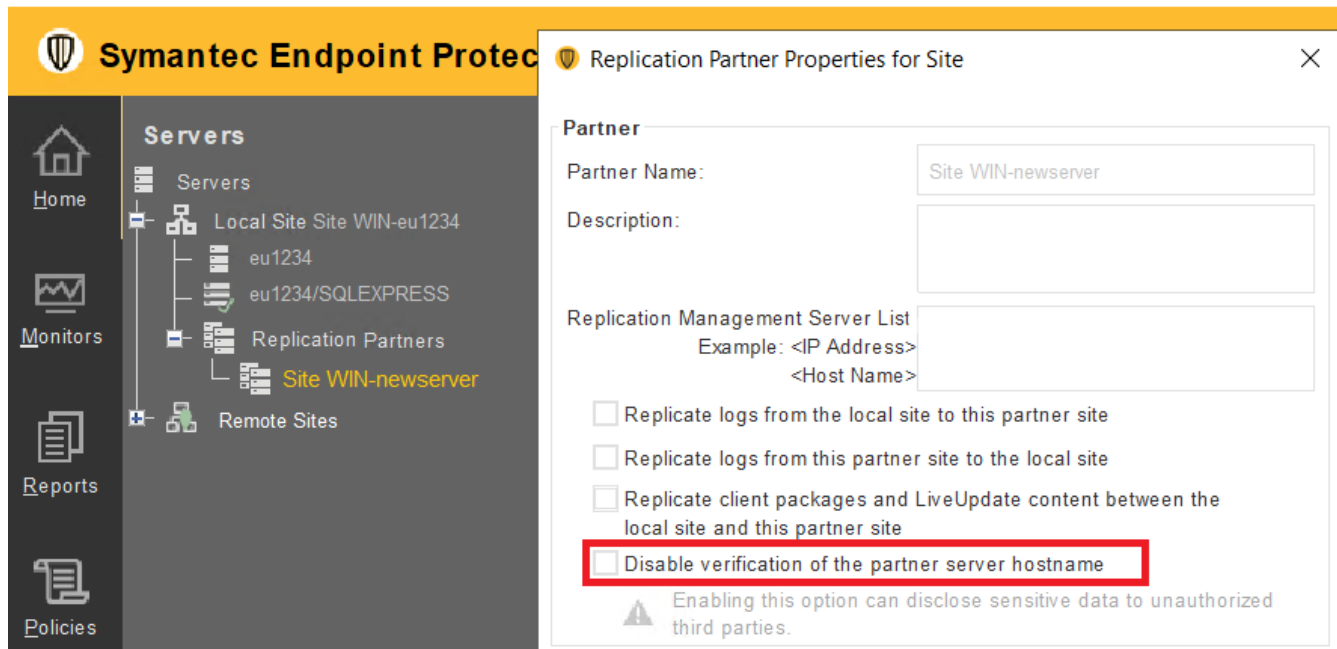
(Optional): To verify that replication runs correctly, right-click the replication partner site and click **Replicate Now**. Wait for the status box that shows the following message: Replication from remote site sitename finished successfully.

[Replicating data immediately](#)

2. Right-click the replication partner site, click **Edit Replication Partner Properties**, clear the **Disable verification of the partner server hostname** option.

This step reenables the verification of the replication partner server host name.

 Symantec Endpoint Protection Manager

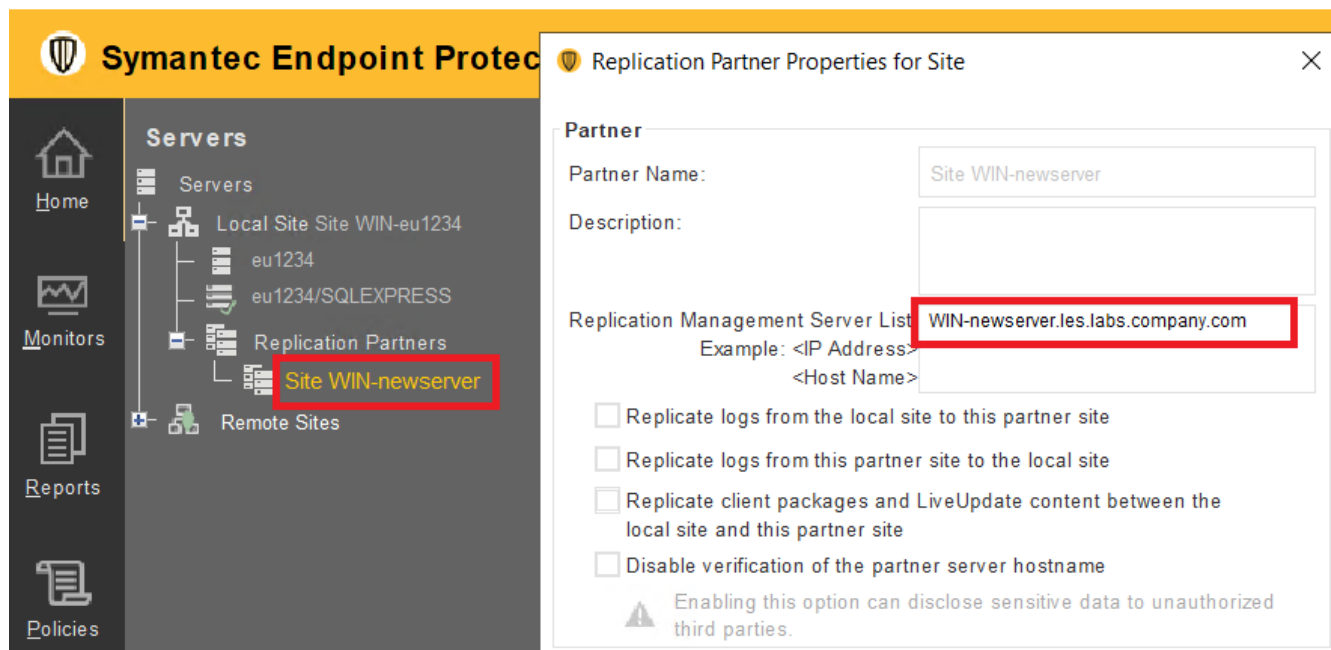


3. On the replication partner server, look at the SAN in the certificate and determine which host name is the correct one for that replication partner server.

There may be multiple SANs. For information about how to find the SAN, see:

[Troubleshooting: Your server certificate is not valid because the computer host name or IP address changed \(14.3 RU8 or later\)](#)

4. On the local management server, click **Admin > Servers > Replication Partners**.
5. Right-click the replication partner site, and click **Edit Replication Partner Properties**.
6. On the **Replication for Partner Properties for Site <Host Name>** tab, paste the replication server host name from step 3 into the **Replication Management Server List** host name field.



7. Click **OK**.
8. (Optional): To verify that replication runs correctly, right-click the replication partner site and click **Replicate Now > Yes > OK**.
9. (Optional): To verify that the replication server trusts the certificate by right-clicking the replication site and clicking **Check Certificate**.
You should see the following message: The certificate is trusted.
10. Repeat these steps for any remaining replication partners.

For information about other certificate verification that you may need to do, see: [Symantec Endpoint Protection Manager has detected that the configured email server or directory server requires certificate verification to be disabled](#)

Troubleshooting: Your server certificate is not valid because the computer host name or IP address changed (14.3 RU8 or later)

When you log on to the Symantec Endpoint Protection Manager, you may see the following error messages.

The following table shows the messages and how to solve the issues.

Version	Message text and solution
14.3 RU9 and later	The server certificate could not be validated. - You rejected the certificate. If you trust the certificate, you must accept it. This message appears because you or an administrator rejected the certificate when prompted to trust it at logon, usually on the remote console. This issue occurs less frequently on the local console, which trusts the server certificate by default. See: Accepting the self-signed server certificate for Symantec Endpoint Protection Manager - You changed the computer hostname or IP address, or updated the server certificate recently. You need to use a valid hostname or IP address that matches your server certificate to log on to the Symantec Endpoint Protection Manager. This message appears after you change the host name or the IP address of the management server computer without also changing the host name or IP address in the certificate. This can also occur when either the management server host name/IP address changed, or a newly imported certificate has a different host name/IP address. See: Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate (14.3 RU9 or later) In 14.3 RU8 and later, Symantec Endpoint Protection Manager verifies whether the computer host name or IP address matches what is listed in the certificate. If the new host names or IP addresses do not match, Symantec Endpoint Protection Manager blocks you from logging on.
14.3 RU8	Your server certificate is not valid because the computer hostname or IP address changed. You need to use a valid hostname or IP address that matches your server certificate to log on to the Symantec Endpoint Protection Manager. The message appears after you change the host name or the IP address of the management server computer without also changing the host name or IP address in the certificate. See: Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate (14.3 RU9 or later)
14.3 RU7 and earlier	Your server certificate is not validated. If you trust the server, you must accept the certificate. Log in again and if the error persists, contact your administrator. You must accept the self-signed certificate when you log on to Symantec Endpoint Protection Manager.

NOTE

The Symantec Endpoint Protection client continues to communicate with the management server.

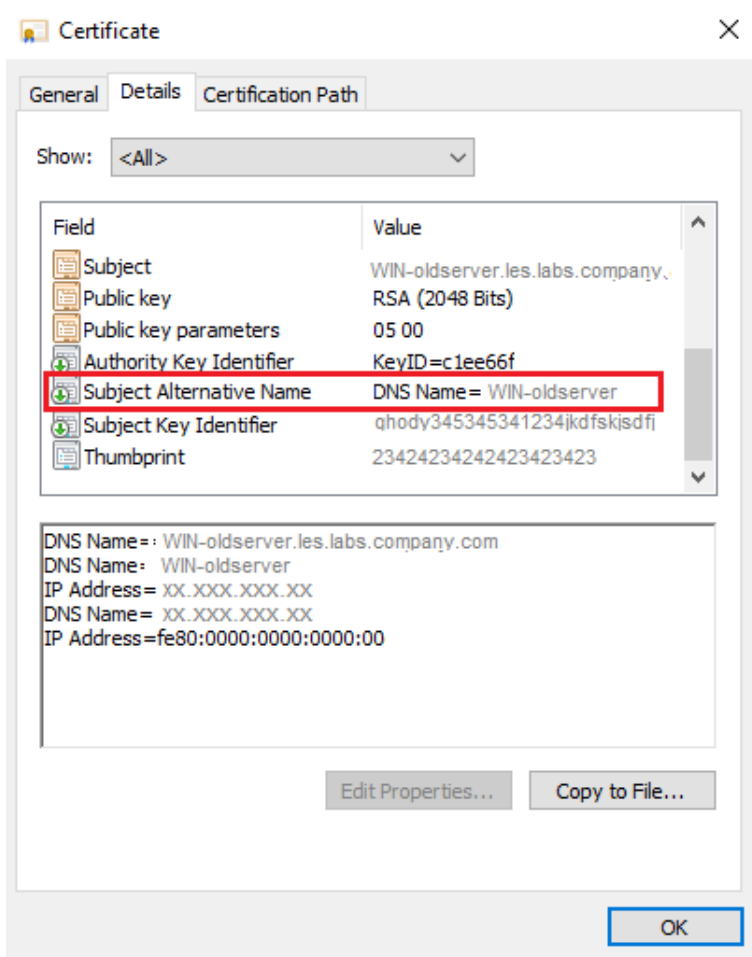
If the host name or IP address from the management server and the certificate do not match, use the following task to log on temporarily to the management server.

NOTE

After you follow this process, make sure that you generate the server certificate and then update the management server name.

To log on to the management server after changing the computer IP address or host name

1. After you change the host name or IP address, restart the management server computer and double-click the `<SEPM_Install>\apache\conf\ssl\server.crt` certificate file.
2. On the **Certificate** dialog box > **Details** tab, copy the values in the **Subject Alternative Name** (host name) or the **IP Address** fields.



3. Open the `C:\Windows\System32\drivers\etc\hosts` file, add `127.0.0.1 <yourHostNameFromServer.crt>`, and save the file.
where `<yourHostNameFromServer.crt>` is the original host name from the `<SEPM_INSTALL>\apache\conf\ssl\server.crt` file from the previous step. In the previous example, the original host name is `WIN-oldserver`.

↑ > This PC > Local Disk (C:) > Windows > System32 > drivers > etc

```
*hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97      rhino.acme.com      # source server
#       38.25.63.10      x.acme.com         # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
127.0.0.1 WIN-oldserver
```

4. On the Symantec Endpoint Protection Manager logon screen, change the new server host name or IP address to the previous management server host name or the IP address, and then log on.
For example, if the original host name is WIN-oldserver and the new host name is WIN-newserver , log on with WIN-oldserver .
5. Generate a server certificate. See:
[Generating a new server certificate](#)
Check that your clients stay connected after you rename or change the IP address.
6. After you update the certificate, log on to Symantec Endpoint Protection Manager using the new host name or IP address.
7. Starting in 14.3 RU9, reconfigure Symantec Endpoint Protection Manager to use the new SEPM host name.
If you see the following error in the **Servers > Local Site > Management Server** status screen: No subject alternative DNS name matching <hostname> reconfigure the Symantec Endpoint Protection Manager.
For example, you would rename SEPM from WIN-oldserver to WIN-newserver .
[Reconfiguring Symantec Endpoint Protection Manager after changing the computer's IP address and host name](#)

Troubleshooting issues when the management server host name changes

Issue	Solution
After you reconfigure the management server so that the server name matches the name in the server certificate, you may see the following error: Error: "Failed to validate the server name in a certificate during Secure Sockets Layer (SSL) initialization." This error occurs if: • The management server uses the default SQL Express database. • You imported a third-party fully qualified domain name (FQDN)-only certificate. This issue occurs because Apache Tomcat does not connect to the SQL Express database.	Follow steps 6 through 8: Reconfiguring the Symantec Endpoint Protection Manager and generating a certificate for the SQL Server Express or SQL Server databases
If the Symantec Endpoint Protection Manager has replication partners, replication may fail. The scm-server-0.log shows one of the following errors. Failed to connect to the specified replication partner server. Verify that the server name and port are correct. Or: <pre>HREAD 28 WARNING: javax.net.ssl.SSLHandshakeException: No subject alternative names matching IP address xx.xx.xx.xx found</pre>	See: • To use a tool to solve this issue: After upgrading Endpoint Protection Manager to 14.3 RU8 replication fails • Login failures and unexpected server errors after upgrading the Endpoint Protection Manager to 14.3 RU8 • For situations where the certificate is only valid for the FQDN: Replication error after upgrade SEPM to Ru8 when using a FQDN only certificate
The management server cannot generate reports and displays the following error: <pre>com.sygate.scm.server.task.SecurityAlertNotifyTask javax.net.ssl.SSLHandshakeException: No subject alternative DNS name matching <servername> found.</pre>	See: Scheduled Reports stop running after upgrading Endpoint Protection Manager to 14.3 RU8

Stopping and starting the management server service

Before you upgrade, you must manually stop the Symantec Endpoint Protection Manager service on every management server in your site. After you upgrade, the service starts automatically.

WARNING

If you do not stop the Symantec Endpoint Protection Manager service before you upgrade the server, you risk corrupting your existing Symantec Endpoint Protection database.

NOTE

If you stop the management server service, the clients can no longer connect to it. If clients are required to communicate with the management server to connect to the network, they are denied access until this service is restarted.

For example, a client must communicate with the management server to pass a Host Integrity check.

For more information, see:

[Upgrading to a new release](#)

To stop and start the management server services using the Control Panel

1. To stop the Symantec Endpoint Protection Manager service, click **Start > Settings > Control Panel > Administrative Tools > Services**.
2. In the **Services** window, under **Name**, scroll to and right-click: **Symantec Endpoint Protection Manager**

Symantec Endpoint Protection ManagerAPI Service

Symantec Endpoint Protection ManagerWebserver

3. Click **Stop**.
4. Close the Services window.

WARNING

Close the Services window or your upgrade can fail.

5. Repeat this procedure for all installations of Symantec Endpoint Protection Manager.

NOTE

To start the Symantec Endpoint Protection Manager service, follow this procedure again, but click **Start**.

To stop and start the management server services using commands

1. To stop the Symantec Endpoint Protection Manager services from a command prompt (cmd), type:

```
net stop semsrv
net stop semapisrv
net stop semwebsrv
```

2. To start the Symantec Endpoint Protection Manager service from a command prompt, type:

```
net start semsrv
net start semapisrv
net start semwebsrv
```

Preventing replication during an upgrade

You should make sure that replication does not occur on any management servers that are configured as replication partners to the management server you are upgrading. If a replication partner launches replication during the upgrade, it may have unpredictable results.

To prevent replication during the upgrade, perform one of the following tasks:

- Reschedule replication to occur outside the upgrade period. Symantec recommends this method as it is simpler.
- Temporarily suspend replication before an upgrade, and restore it after the replication is over.

Rescheduling replication

The advantage to modifying the schedule is that the other sites do not replicate, and they keep servicing the clients until the clients are upgraded. After the upgrade finishes, the sites can both test replication by forcing a one-time replication and change the schedule back to the previous set schedule and frequency.

Follow these best practices to modify the schedule:

- Document existing schedule and settings.
- Change the schedule to prevent replication from happening during upgrade window by scheduling it in the future or different day.
- Force replication so that schedule is picked up by all replication partners, or sites.

For more information, see:

[Changing the replication frequency and content](#)

Suspending and restoring replication

You must log on to Symantec Endpoint Protection Manager and suspend replication at a minimum of two sites.

WARNING

Suspending replication is not the same as permanently deleting the replication partnership. If you delete the relationship and then reinstall the management server, the management servers perform a full replication instead of an incremental replication. See: [Deleting sites](#)

To suspend and restore replication

1. In the console, click **Admin > Servers**.
2. Under **Local Site > Servers**, expand **Replication Partners** and select the management server.
3. Right-click the management server, and then click **Delete Replication Partner**.
4. Click **Yes**.
5. Repeat this procedure at all sites that replicate data.
6. Restore replication and restart the management server service. See: [Restoring replication](#)

More information

- [Upgrade best practices for Endpoint Protection 14](#)
- [Upgrading to a new release](#)

Restoring replication

After you upgrade all management servers that had a replication relationship, you add the replication partner back. You must also re-add the management servers that were configured for failover and load balancing.

You only re-add replication partners on the computer on which you first upgraded the management server. The upgraded management server must also have previously been a replication partner in the same site farm.

After you add the replication partner back, Symantec Endpoint Protection Manager makes the databases consistent. However, some changes may collide. See:

[How to resolve data conflicts between sites during replication](#)

If you have two separate, non-replicating sites, you can also use this option to convert one of the sites into a site which replicates with the other site.

To restore replication

1. On the console, click **Admin > Servers**.
2. Under **Servers**, expand **Local Site**, and under **Tasks**, click **Add Existing Replication Partner**.
3. In the welcome panel, click **Next**.
4. In the **Remote Site Information** panel, type the IP address or host name for the second management server, the system administrator's logon information, and then click **Next**.
The system administrator's user name is `admin` by default.
5. Set the replication schedule and click **Next**.
6. Check which items to replicate, and then click **Next**.
Client package replication uses large amounts of traffic and hard disk space.
If you click **Yes**, the management server performs a full replication of data between the two replication partners.
7. When a message appears asking whether or not you have restored the database on the partner site, click one of the following options:
 - Click **No** to replicate only the data that changed since this partner relationship was disabled. Symantec recommends this option, especially if your network has low bandwidth.
 - Click **Yes** to perform a full replication of data between the two replication partners.
8. Click **Finish**.

9. Repeat this procedure for all computers that replicate data with this computer.
Make sure that you restart the management server service after you restart replication.

More information

- [Upgrade best practices for Endpoint Protection 14](#)
- [Upgrading to a new release](#)

Choosing which method to upgrade the client software

You can upgrade the client using multiple ways. The method you should use depends on your environment and goals. For example, you might have a large number of clients or groups, or computers that run different versions of the client.

Some methods can take up to 30 minutes. Therefore, you may want to upgrade client software when most users are not logged on to their computers.

Table 52: Methods to upgrade the client software

Method	When to use	When not to use
AutoUpgrade (Recommended for smaller environments)	• When you have a smaller number of clients, such as 5,000 clients or fewer. • When you need to schedule the upgrade to occur when the upgrade does not interrupt the users' work. • When you use Symantec Endpoint Protection Manager and not a third-party application to deploy the client installation package. • When you need to upgrade either Windows or Mac clients, but not Linux clients. • When you want a simple upgrade method. For more information, see: Upgrading client software with AutoUpgrade	• When you have a larger number of clients. This method does not scale well. • When you have a lot of groups, because it is time-consuming to click each group individually in the wizard. • When you have a complicated upgrade schedule where you need a lot of granularity. • When you need to upgrade Linux clients. See: How to deploy the Symantec Endpoint Protection Linux client as part of a cloned drive image
Export a client installation package (Recommended for larger environments)	• When you deploy the client installation package manually instead of with Symantec Endpoint Protection Manager. • When you deploy the client installation package with an existing third-party deployment application instead of with Symantec Endpoint Protection Manager. To use this method, you should have this infrastructure already in place. • When you need to upgrade Windows clients, Mac clients, and Linux clients. For more information, see: • Exporting client installation packages • Installing Windows client software using third-party tools	When you normally use Symantec Endpoint Protection Manager to update the clients.
Client Deployment Wizard	• When you have a smaller number of clients, such as fewer than 250 clients. • When you deploy the client using Symantec Endpoint Protection Manager and not a third-party application. • When you want a simpler upgrade method. Use the New Package Deployment . See: Installing Symantec Endpoint Protection clients with Remote Push	When you have a large network environment, as this method does not scale well.

Method	When to use	When not to use
Download client installation files from the Broadcom Download Management page.	- When you want to upgrade a few clients at a time in a few specific cases. For example: - If an issue occurs on a few computers with an older version of the client, and the newer version fixes the issue. - If you have a smaller number of clients to upgrade and do not want to upgrade the management server. - When you need to upgrade Windows, Mac, and Linux clients. - When you must deploy the client directly on the computer or by using a third-party deployment application instead of Symantec Endpoint Protection Manager. You download the standalone All Clients installation file from the Download Management page. To do this: - Go to: Symantec Getting Started - Select On-Premises Security Products. For more information, see: Installing an unmanaged Windows client	If you upgrade the client on computers with existing managed clients, the clients stay managed. However, if you deploy to new computers without an existing client, this method installs an unmanaged client only. You must convert the client to a managed client later to connect to the management server. See: How do I replace the client-server communications file on the client computer? Exporting the client-server communications file (Sylink.xml) manually

More information

[Upgrading to a new release](#)

Upgrading client software with AutoUpgrade

Overview

AutoUpgrade lets you automatically upgrade the Symantec Endpoint Protection client software on the Windows or Mac clients in a group.

With AutoUpgrade, Windows standard clients receive a delta upgrade package that Symantec Endpoint Protection Manager creates. This package is smaller than the full installation package. Windows that are embedded or VDI clients always receive the full installation package. These clients do not maintain a copy of the installer in the installer cache. Mac clients always receive the full installation package.

AutoUpgrade Best Practices

Use the following best practices for using AutoUpgrade:

- Test the AutoUpgrade process before you attempt to upgrade a large number of clients in your production network. If you do not have a test network, you can create a test group within your production network. For this kind of test, you add a few non-critical clients to the test group and then upgrade them by using AutoUpgrade.
- To reduce bandwidth during peak hours, schedule AutoUpgrade for after hours in the **Upgrade Clients with Package** wizard, especially for client groups with reduced-size clients. For wide area networks, you should also set up the remote clients to receive the upgrade package from a remote web server.
- As of 14.3 RU2, LiveUpdate downloads client installation packages with critical fixes or security fixes that you can install without a change to the client version. For example, if you had installed 14.3 RU2 build 4870, and 14.3 RU2 build 5200 becomes available, you use the AutoUpgrade wizard to install build 5200. You do not need to upgrade the management server; just the clients. You must restart the 14.3 RU2 and earlier clients after each upgrade. For 14.3 RU3 and later, see: [Restarting the client computers from the Symantec Endpoint Protection Manager](#)
- In 14.3 RU2 and 14.3 RU3, both the Symantec Endpoint Protection clients and the Symantec Endpoint Protection Manager were localized in the following languages only: English, French, Spanish, Portuguese, and Japanese. In 14.3 RU4, SEP added Simplified and Traditional Chinese. If you are using one of the supported languages, no action

is required; you can upgrade as usual. You can automatically upgrade the client language to English if the previous client's language is unavailable. If you choose a non-English language, the clients with an unsupported language do not get upgraded. This option is off by default. To enable this option, click **Clients** page > **Install Packages** page, click **Add a Client Install Package** > **Upgrade to English if unsupported language is unavailable**. This option applies to the Windows client only.

[Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language](#)

- Since AutoUpgrade was first included in the Mac client with Symantec Endpoint Protection 14, you cannot upgrade with AutoUpgrade from a version earlier than 14.
- After you upgrade Symantec Endpoint Protection Manager, run LiveUpdate in the console at least once before you use AutoUpgrade to upgrade the clients.

[Checking that Symantec Endpoint Protection Manager has the latest content](#)

- AutoUpgrade can only install the Application Hardening feature (14.2 and later) on client computers when the following conditions are met:
 - You must enable **Maintain existing client features when updating** when you run **Upgrade Clients with Package**. This setting is enabled by default.
 - The client computer cannot have the Symantec Data Center Security agent installed.
 - The Virus and Spyware Protection feature is currently installed and selected for upgrade.
- If you want to change between the Windows client installation types: **Standard client**, **Embedded or VDI**, **Dark network**, at a later time after client installation, you **must** first uninstall the existing client software, reconfigure these settings, and then reinstall the new client package. You cannot change this setting using AutoUpgrade.

To upgrade client software with AutoUpgrade

1. In the console, click **Admin** > **Install Packages**.
2. Under **Tasks**, click **Upgrade Clients with Package**.
3. In the **Upgrade Clients Wizard** panel, click **Next**, select the appropriate client installation package, and then click **Next**.
4. Select the group or groups that contain the client computers that you want to upgrade, and then click **Next**.
5. Select from where the client should download the package from the following options:
 - To download from the Symantec Endpoint Protection Manager server, click **Download from the management server**.
 - To download from a web server that is local to the computers that need to update, click **Download from the following URL (http or https)**. Enter the URL of the client installation package into the provided field.
6. Click **Upgrade Settings** to specify upgrade options.
7. On the **General** tab, under **Client Settings**, choose from the following options, depending on the client operating system:
 - For Windows:
 - In the **Select the version for this package** to choose a build (as of 14.3 RU2).
 - Use the drop-down menus to select options for **Maintain existing client features when updating** and **Install Settings**. If you deselect **Maintain existing client features when updating**, you can optionally add or remove features when upgrading.
 - For Mac, use the drop-down menu to select options for **Install Settings**.
 - For Windows, **Content Selection** lets you include content in the installation package. If you include content, the package is larger, but the client has up-to-date content immediately after installation. If you do not include content, the package is smaller, but the client must get content updates after installation.

You can also add an optional upgrade schedule. Without a schedule, the AutoUpgrade process begins after the wizard completes.
8. On the **Notification** tab, customize the user notification settings.

You can customize the message that is displayed on the client computer during the upgrade. You can also allow the user to postpone the upgrade.
9. Click **OK**, and then click **Next**.

10. In the **Upgrade Clients Wizard Complete** panel, click **Finish**.

To confirm the version number of the client software

1. After the upgrade completes, you can check the version to confirm a successful upgrade in one of the following ways:
 - In the console, click **Clients > Clients**, select the appropriate group, and change the view to **Client Status**.
 - On the Windows client, in the Symantec Endpoint Protection client interface, click **Help > About**.
 - On the Mac client, open the Symantec Endpoint Protection client interface. In the menu bar, click **Symantec Endpoint Protection > About Symantec Endpoint Protection**.

By default, the clients restart after installation. For 14.3 RU2 and earlier clients, the computer must restart after the upgrade. You can configure the restart options in the group's general settings to control how the clients in a group restart after AutoUpgrade. You can also restart the clients at any time by running a restart command from the management server.

[Restarting the client computers from Symantec Endpoint Protection Manager](#)

[Applying upgrade settings to other groups](#)

Configuring the Client Upgrade policy (Optional)

As of 14.3 RU3, you can upgrade a subset of the clients within a security group on different days for a measured rollout. You use the Client Upgrade policy and the following location conditions to target these subgroups: host name, user name, group name, whether a file exists, or operating system. For example, you can upgrade Windows 8 computers in the middle of the night when users are offline.

The Client Upgrade policy provides more granular schedule settings that overrides the upgrade schedule settings in the AutoUpgrade wizard. The policy retains all other AutoUpgrade wizard settings. You apply the Client Upgrade policy to the same group to which you apply the AutoUpgrade wizard.

[Upgrading client software with the Client Upgrade policy](#)

Applying AutoUpgrade settings to other groups

You can copy existing AutoUpgrade client installation package upgrade settings from one group to another group. If you copy upgrade settings, you don't have to create the package settings for each group individually.

This option copies the following client install package settings:

- The client feature set
- Whether **Maintain existing client features when updating** is enabled or disabled
- The client installation settings
- The content selection
- The download source
- The upgrade schedule
- The settings and message text from the **Notifications** tab

The Windows settings apply to Windows clients and the Mac settings apply to Mac clients during AutoUpgrade. They also apply to any new client that joins the group.

If you apply the copied settings to a package that is already assigned to a target group, the copied settings override the target group's existing settings. If the target group has no assigned package, this option adds a client install package with the copied settings.

To apply upgrade settings to other groups

1. In the console, do one of the following tasks:
 - Click **Clients > Install Packages**, select the group, and under **Tasks**, click **Apply current deployment settings to other groups**.
 - Click **Clients**, right-click a group, and then click **Copy Deployment Settings**.
2. In the **Copy Deployment Settings** dialog box, click the new groups, click **OK**, and then click **Yes**.

More information

[Upgrading client software with AutoUpgrade](#)

Upgrading client software with the Client Upgrade policy

You can distribute and install an upgrade package to a subset of clients within the client group (14.3 RU2 clients and later). The Client Upgrade policy lets you schedule the upgrade over multiple days and times. This staggered upgrade lets you release the software at a predetermined time and helps you test the upgrade before you roll it out to all clients.

Use locations to specify which conditions a client must meet to upgrade with the new schedule. For example, you can upgrade Windows 10 computers on the weekend when users are offline.

When do I use the Client Upgrade policy?

The Client Upgrade policy provides more advanced scheduling options beyond the AutoUpgrade wizard. The policy runs on groups for which you have already configured AutoUpgrade.

The following table describes the differences between the AutoUpgrade wizard alone versus the additional Client Upgrade policy.

Table 53: AutoUpgrade wizard versus the Client Upgrade policy

AutoUpgrade wizard only	Client Upgrade policy
For Windows clients version 14.3 RU2 MP1 and earlier. These clients ignore the Client Upgrade policy settings and obtain their schedule settings from the General tab > Upgrade Schedule settings in the AutoUpgrade wizard. You can find the upgrade schedule settings in the client's default location for the config.xml file: C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\.	For Windows clients 14.3 RU2 and later clients. These clients ignore the AutoUpgrade wizard schedule settings; all other AutoUpgrade settings apply.
Specifies the start and end time of the upgrade and the number of days over which the download package is distributed.	Specifies: • The start and end time of the upgrade. • The number of days over which the download package is distributed. • Which days of the week to upgrade. • How many days the upgrade can delay. • Ability to retry the upgrade if it gets missed during the distribution time period.
Does not use location awareness	Lets you upgrade a subset of clients by using the following locations awareness conditions: host name, user or group name, a specified file, or operating system. Location awareness provides better options for clients in low-bandwidth environments.
Upgrades Windows and Mac clients but not Linux clients.	Upgrades Windows clients but not Mac or Linux clients.

Downloads and installs a full client installation package from the Symantec Endpoint Protection Manager, Group Update Provider, or LiveUpdate.	Downloads and installs a full client installation package from the Symantec Endpoint Protection Manager, a Group Update Provider, but not LiveUpdate.
Downloads any client product updates or client patches from LiveUpdate, including a production LiveUpdate or LiveUpdate Administrator.	Does not download any client product updates or client patches from LiveUpdate. Client patches use the schedule in the LiveUpdate Settings policy.
Downloads and installs the Symantec Agent package that the Symantec Endpoint Security cloud console manages.	Does not download and install the Symantec Agent package that the Symantec Endpoint Security cloud console manages.

Configuring the Client Upgrade policy

Step 1: Assign a client installation package to a group using the AutoUpgrade wizard

Configure and assign a client installation package to the client group. You can accept the default **Upgrade Schedule** settings.

[Upgrading client software with AutoUpgrade](#)

Step 2: Create multiple locations for the group

Set up location awareness so that clients switch to a location that directs the clients to upgrade.

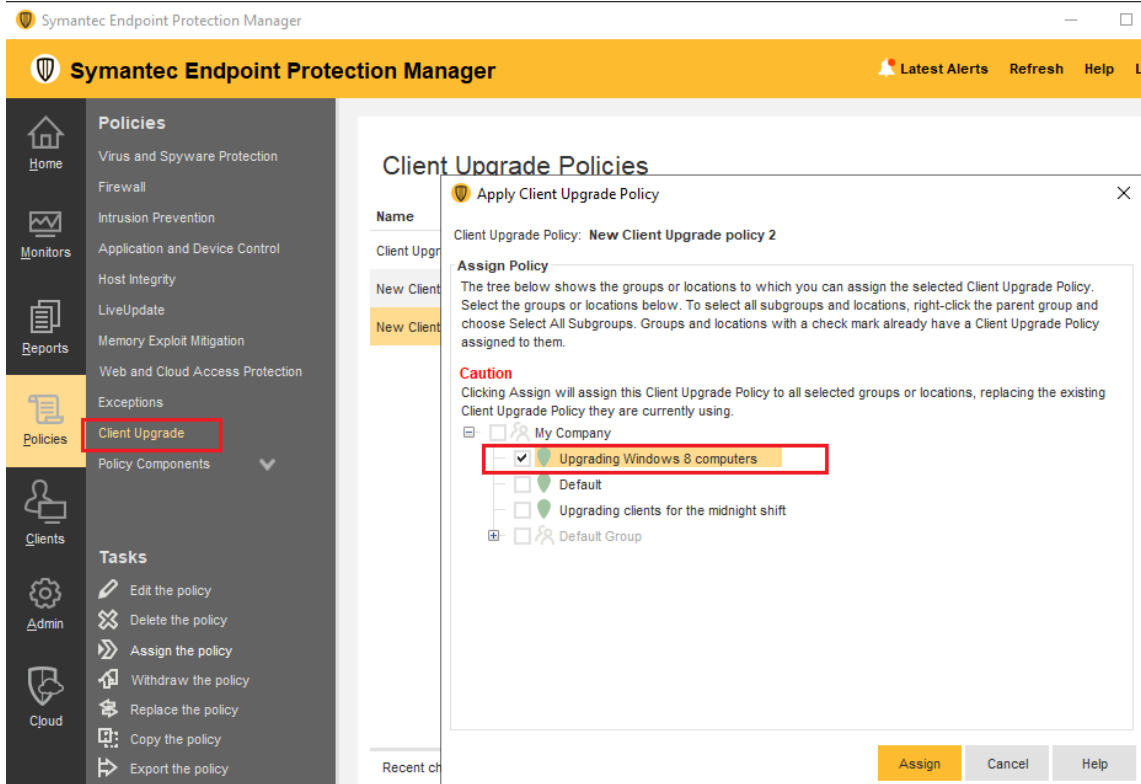
1. In the console, click **Clients > Policies**, and select the group.
2. On the **Policies** tab, click **Manage locations** and add a location using any of the following criteria: Host name, user name, group name, file exists, or operating system.

[Adding a location to a group](#)

[Specify Location Criteria](#)

Step 3: Create the Client Upgrade policy and assign it to a location

1. In the console, click **Policies > Client Upgrade** to create a Client Upgrade policy.
2. In the **Overview** pane, click **Enable this policy**.
If you do not enable the Client Upgrade policy, the clients use the upgrade schedule options in the client installation package you added in Step 1.
3. In the **Schedule** pane, specify the following recommended options:
 - **Upgrade from...to**
 - **Allow upgrades**
 These options set the frequency for how often the management server checks for a new client upgrade package and downloads it to the clients.
4. Click **OK** and assign the policy to one of the locations you created in Step 2.



After the management server downloads the policy.xml file to the clients, the clients switch locations.

The clients upgrade based on the schedule you specified in the Client Upgrade policy.

Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language

If you upgrade the client or SEPM from an unsupported language, you upgrade to either a supported language or English.

In 14.3 RU1 and earlier, both the Symantec Endpoint Protection Manager (SEPM) and the clients supported 12 languages. In later releases, language support that is changed as follows:

- In 14.3 RU2, language support was reduced to English, Brazilian Portuguese, French, Japanese, and Spanish.
- In 14.3 RU4, SEP added Simplified and Traditional Chinese.
- In 14.3 RU5, SEP added Czech, Polish, and Russian.

Upgrading the Symantec Endpoint Protection Manager from a supported to an unsupported language

When you upgrade a SEPM with an unsupported Symantec Endpoint Protection Manager language, SEPM is automatically upgraded to English. However, you can upgrade SEPM to a supported language other than English, such as from Italian to French.

SEPM uses two components to display a language: the resource files and the system locale settings. To display SEPM in one of the supported languages other than English, SEPM must have both the resource file and the system format locale setting in the same language. If the resource file and the system locale setting do not match a supported language, SEPM is installed in English.

NOTE

Symantec recommends you follow this step before you upgrade the management server.

To set the system format locale to the target migration language

1. Click the **Start -> Control Panel -> Clock and Region -> Region -> Formats** tab (Windows 10 and Windows Server 2019).

This step changes depending on which Windows version that SEPM runs on.

2. In the **Format** drop-down list, choose the target language, and then click **OK**.

You can choose any format for the target language. For example, if you want to upgrade to French, it makes no difference if you choose French (Algeria) or French (Belgium).

Upgrading the clients from an unsupported language to a supported language

To automatically upgrade clients with an unsupported language to English, check the **Upgrade 14.3+ clients to English if client language is not a supported** option in the AutoUpgrade wizard. If you uncheck this option, clients with an unsupported language do not upgrade automatically. This option is available in an English Symantec Endpoint Protection Manager only.

Mac: Mac clients must be upgraded from an unsupported language to a supported language manually or using desktop management tools.

Linux: The Linux client remains translated into Japanese only.

NOTE

If you automatically upgrade a client with an unsupported language to English, the client continues to display the date settings for definitions in English (14.3 RU1 and later). To work around this issue, uninstall the legacy client and manually install a new client installation package. In addition, a fix is expected for clients that are upgraded automatically. [SEP-72481]

For more information, see:

[Upgrading client software with AutoUpgrade](#)

Installing Endpoint Protection client patches on Windows clients

What are client patches and how do they work?

A client patch is a software patch for Symantec Endpoint Protection Windows clients that corrects a product defect or functionality issue that exists in the client code. Symantec delivers a client patch to fix the issue and uploads it to a LiveUpdate server in 14.3 RU2 (build number 14.3.4615.2000) or later. Client patches are like any other type of content, like IPS signatures or virus and spyware definitions.

You download client patches from the LiveUpdate server to the management server as an incremental delta (.dax) file. You then download the patches to clients in the same way as other content, using a LiveUpdate server, the management server, or a Group Update Provider (GUP). See:

[Choose a distribution method to update content on clients](#)

NOTE

A client patch is not the same as a maintenance patch (MP) or a release update (RU). A client patch only addresses a client defect, and is delivered through LiveUpdate. A maintenance patch provides other updates or features, such as to offer support for new operating systems, and is delivered as a full installation download through the Broadcom [Download Management](#) page. In 14.3 RU2 and later, client patches have the same content as product updates. However, product updates are included in a full client installation package, whereas a client patch includes just the delta file. See:

[About Endpoint Protection release types and versions](#)

See also:

Upgrading client software with AutoUpgrade

How do client patches work with languages?

The language for client patches must match the management server language. For example, a French management server that manages French (supported) and German (unsupported) clients provides client patches to the French clients only. In 14.3 RU2 or later, you must enable AutoUpgrade to install an English installation package and English client patches on the German client. For more information about how to upgrade clients from an unsupported language to a supported language, see:

[Upgrading Symantec Endpoint Protection 14.3 RU2+ to a supported language](#)

Installing client patches on Windows computers

By default, LiveUpdate downloads client patches to Symantec Endpoint Protection Manager. However, client patches do not automatically download and install on either a managed client or an unmanaged client. On the managed client, you must select the client patch to install it, whether you use the Symantec Endpoint Protection Manager, LiveUpdate, or a Group Update Provider.

After a client downloads and installs a client patch, the patch runs immediately (14.3 RU2 and later). For 14.3 RU1 and earlier, it continues to run the previous, unpatched version of the client until the client is restarted. Either the client end user must restart the computer, or you must run the restart command from the management server. The management server sends you a notification that indicates which clients require a restart. See:

[Restarting the client computers from the Symantec Endpoint Protection Manager](#)

NOTE

Like client installation packages, you cannot roll a client patch back. You must uninstall and reinstall a client installation package from the previous release.

To install client patches on Windows clients

1. In the console, verify that LiveUpdate is configured to download the client patches to the management server. In the **Content Types to Download** dialog box, make sure that **Client patches** is checked. See:
[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)
2. To run a report to find out which release is installed on the client computers, run a **Protection Content Versions** report. See:
[Generating a list of the Symantec Endpoint Protection versions installed in your network](#)
3. Verify that the LiveUpdate Settings policy is configured to download the patches to the clients. In a LiveUpdate Settings policy, under **Windows Settings**, click **Advanced Settings**. Make sure **Download client patches** is checked.

NOTE

Make sure that **Download delta content from a LiveUpdate server when available** is checked. This option merges the client patches from the current release with the content with the new patch, and then downloads only the difference, or the delta. Use this option when bandwidth to the clients is low.

4. Restart the client computers. See:
[Running commands on client computers from the console](#)

Upgrading the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux

Upgrade your SEP Linux Agent or the Symantec Single Agent for Linux agent to the most current version to get new functionality and the latest security enhancements.

NOTE

Both the Symantec Single Agent for Linux and the Symantec Endpoint Protection Linux Agent are referred to in this topic as the Linux Agent.

For RU8 and later:

As of version 14.3 RU1, the Linux client installer detects and uninstalls the legacy Linux client (earlier than 14.3 RU1) and then performs a fresh install. Old configurations will not be retained.

To upgrade the Symantec Linux Agent

1. In Symantec Endpoint Protection Manager, create and download the installation package.

[Exporting client installation packages](#)

2. Copy the downloaded package to the Linux device.
3. Navigate to folder location and run the following command to make the **LinuxInstaller** file executable:

```
chmod u+x LinuxInstaller
```

4. Run the following command to uninstall the existing agent and re-install the Symantec Linux Agent:

```
./LinuxInstaller
```

Run the command as root.

5. To verify the installation, navigate to `/usr/lib/symantec`. Run the `./status.sh` script to confirm that the modules are loaded and daemons are running:

```
./status.sh
Symantec Agent for Linux Version: 14.3.450.1000
Checking Symantec Agent for Linux (SEPM) status..
Daemon status:
cafagent           running
sisamdagent        running
sisidsagent        running
sisipsagent        running
Module status:
sisevt             loaded
sisap              loaded
```

Updating the kernel modules for Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux

Update the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux with the most recent Linux kernels, when available. Updates can contain fixes, security enhancements, better hardware compatibility, improved stability, and new features.

NOTE

Both the Symantec Single Agent for Linux and the Symantec Endpoint Protection Linux Agent are referred to in this topic as the Linux Agent.

The Linux Agent is the same client whether you manage it from the Symantec Endpoint Protection Manager or the cloud console.

Click here for the [Supported kernels of Symantec Linux Agent](#).

Broadcom validates each version of the Symantec Endpoint Protection Linux Agent with specific Linux kernel modules. You must ensure that your kernel module (KMOD) is matched by consulting the support matrix.

Whenever a new Linux kernel module update is released, the Linux Agent for that platform must be updated to support the new kernel. KMODs can also be updated by using the Linux repository online, or offline methods.

NOTE

Ensure that the agents can connect to the Symantec repository server (<https://linux-repo.us.securitycloud.symantec.com/>) to download the kernel module updates.

Whenever you run the `yum update` command on a RHEL, Amazon Linux, Oracle Linux, or CentOS system, the command also looks for new agent packages. If an update is available, the latest kernel module is downloaded and the agent is updated automatically. After the kernel module is updated, you must restart the instance for the update to take effect.

Alternatively, you can update the agent kernel module by running the following command in the instance. Open a terminal window with root privileges, navigate to `/usr/lib/symantec/` and run the following command:

```
/usr/lib/symantec/installagent.sh --update-kmod
```

To update kernel modules on Ubuntu systems

1. To refresh and update local package database, type the following commands:

```
sudo apt-get clean
sudo apt-get update
```

2. To upgrade to the latest kernel module, type the following commands:

```
/usr/lib/symantec/installagent.sh --update-kmod
```

Superuser privileges are required to perform this action.

To update kernel modules in a restricted environment with no Internet connection

1. Method 1: Manually transfer the latest KMOD package to a system that has no Internet connection, attach the KMOD package to the LinuxInstaller, and then run the LinuxInstaller.

1. On a system that has Internet connection, download the KMOD package.

```
./LinuxInstaller -d
```

2. Manually copy and paste the KMOD package to the agent that you want to upgrade.

3. List the attached packages.

```
./LinuxInstaller -l
```

4. Attach the new KMOD package to the LinuxInstaller.

```
tar czf - [KMOD-package-name] >> LinuxInstaller
```

5. Make sure that the new KMOD package is included in the list of attached packages.

```
./LinuxInstaller -l
```

6. Run the installer to update the kernel modules.

```
./LinuxInstaller -- --update-kmod
```

2. Method 2: Set up a local repository and edit the repository settings so that the agent uses the local repository instead of the default Symantec repository.

1. Set up the local repository that hosts the KMOD packages.

For information about how to create a local repository, refer to documentation of the respective Linux distribution that you are using.

2. On the client computer, run the following command to redirect it to use the local repo:

```
./LinuxInstaller --local-repo <localrepo_url>
```

Example of the URL: `--local-repo 'http://<repo_ip_or_hostname:<port_optional>/sep_linux'`

3. To update the KMOD, run:

```
./LinuxInstaller -- --update-kmod
```

If you update the operating system kernel module, you must also update the corresponding kernel module update for the Symantec Endpoint Protection client. Without the compatible kernel module, the Symantec Endpoint Protection client may not work properly and some features may be disabled.

[Creating and installing a Symantec Linux Agent installation package](#)

Upgrading Group Update Providers

Use this procedure to upgrade the clients that are Group Update Providers.

To upgrade Group Update Provider clients

1. Upgrade the Symantec Endpoint Protection Manager server to the new version of the software.
2. Upgrade the clients that are Group Update Providers to the new version of the client software.
3. Update the rest of the clients to the new version of the client software.

More information

- [Using Group Update Providers to distribute content to clients](#)
- [Upgrading to a new release](#)

Migrating to the SES cloud console

Learn how to move the management of your client computers from the on-premises Symantec Endpoint Protection Manager (SEPM) to the Symantec Endpoint Security (SES) cloud-based console.

How do on-premises features and cloud features compare?

There are many [benefits](#) to moving to Symantec Endpoint Security.

Explore a high level comparison of [features](#) that SES has to offer.

For a detailed comparison, see: [Feature comparison between the on-premises Symantec Endpoint Protection and Symantec Endpoint Security Complete](#)

Before you begin

Choose the [management option](#) that's best for your organization and supported by your product type and license.

Review this [important information](#) and make sure that your environment meets the [prerequisites](#).

[FAQs about moving to Symantec Endpoint Security \(SES\) from Symantec Endpoint Protection \(SEP\)](#)

Does a SES license work on SEP?

The Symantec Endpoint Security license works with all three management options. The Symantec Endpoint Security Complete (SESC) license gives you more protection technologies than the Symantec Endpoint Security Enterprise (SESE) license.

How to move to SES

Follow the workflow for migrating to the management option that you chose.

Migration option	More information
On-premises to hybrid	• Symantec recommends that you first test the cloud console with the hybrid-management default SEPM domain into the cloud server. – Enrolling a Symantec Endpoint Protection Manager domain into the cloud server – Enrolling a Symantec Endpoint Protection Manager domain with the cloud server (1
Hybrid to cloud	After a test period, move from the hybrid mode all the way to the fully native cloud option. Moving from the hybrid-managed Symantec Endpoint Protection Manager (SEPM) option option
On-premises to cloud	Or, go directly from on-premises to fully cloud-managed. This approach is simpler and provides a hybrid approach. Moving directly from an on-premises Symantec Endpoint Protection Manager (SEPM) option option

When the move is complete

If you are using Symantec Endpoint Security for the first time, see: [Getting started with Symantec Endpoint Security](#)

Benefits of moving to the Symantec Endpoint Security cloud console

Migrating from an on-premises solution to a cloud solution has many benefits.

Benefits of moving to the cloud

Regardless of the management option that you chose (hybrid or fully cloud managed), you get the following benefits from managing the clients in your organization from the Symantec Endpoint Security (SES) cloud console:

- No cost or overhead of installing and managing a management server and database.
- Capability to share management of multiple Symantec enterprise products across a single management console.
- Unified visibility into threats, policies, and incidents from multiple Symantec products, which reduce incident response times from days to minutes.
- Improved console for administration and visibility.
- Dynamic platform with monthly updates.
- Automatic client upgrade.

Benefits to a hybrid managed option

Symantec recommends that you test the cloud console first before moving fully to the cloud console.

With the hybrid managed option, you can manage your clients and some policies from Symantec Endpoint Security. You manage other policies from the Symantec Endpoint Protection Manager. This hybrid-managed option provides some additional security features that the on-premises Symantec Endpoint Protection Manager does not provide.

To use hybrid management, you enroll each Symantec Endpoint Protection Manager domain in the SES cloud server.

The following list is a high-level summary of the features that you get when you enroll a Symantec Endpoint Protection Manager domain:

- Manage unusual or risky behavior by trusted applications with the Adaptive Protection policy
- Detect and expose suspicious network activity with Endpoint Detection and Response.
- Integrated false positive management with a central allow list and deny list
- Modern cloud console for managing advanced features

More information

[Choosing between the on-premises management, hybrid management, or cloud management options](#)

Benefits to a fully cloud-managed option

Symantec Endpoint Security has features that the Symantec Endpoint Protection Manager on-premises console does not have:

- Endpoint Detection and Response (EDR)
- Adaptive Protection
- App Control
- Threat Defense for Active Directory
- Antimalware
- Mobile Threat Defense and Secure Connection

NOTE

You get the most features with the Symantec Endpoint Security Complete subscription rather than the Symantec Endpoint Security Enterprise subscription.

More information:

- [Supported Symantec Endpoint Security features by Symantec Endpoint Protection deployment type](#)
- [What is Symantec Endpoint Security?](#)
- [Symantec Endpoint Security Complete](#)

On-premises, hybrid, or fully cloud management options

You can manage the agents from the on-premises Symantec Endpoint Protection Manager (SEPM) only, the Symantec Endpoint Security (SES) cloud console only, or a combination of both (hybrid management).

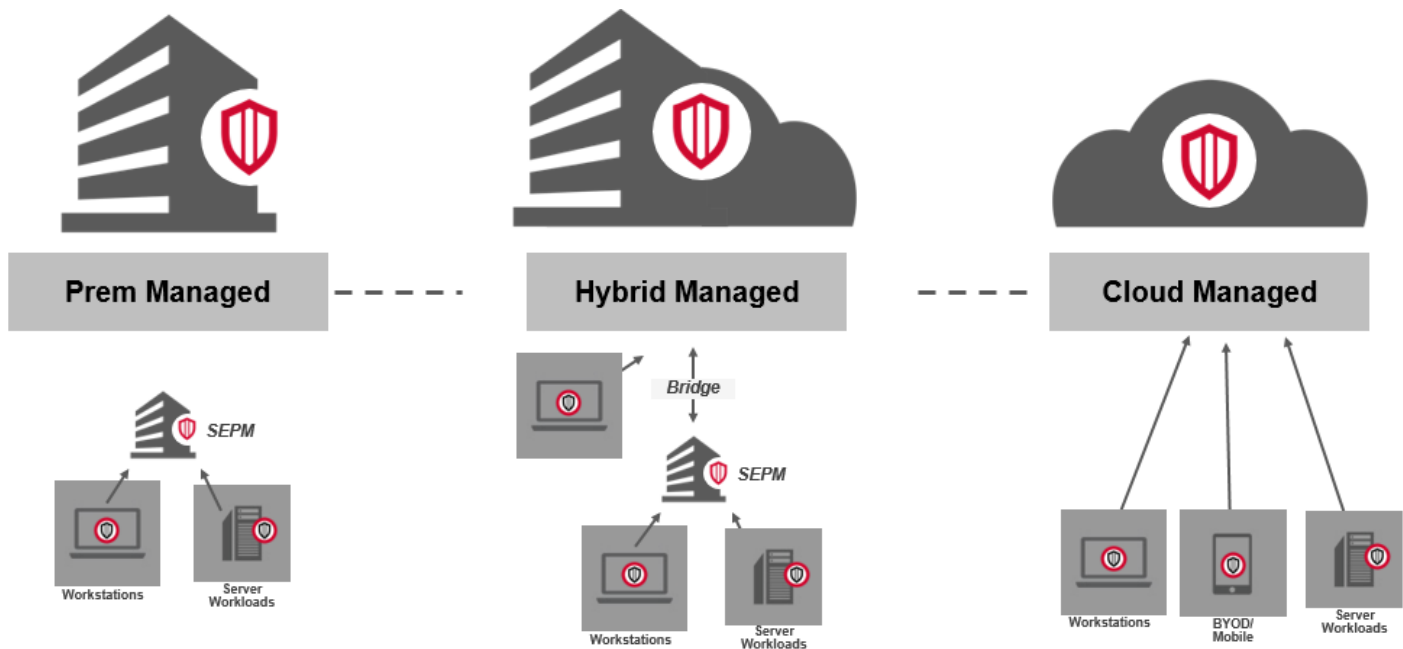


Table 54: Differences between each management choice

	On-premises	Hybrid	Native cloud
License	Symantec Endpoint Protection or Symantec Endpoint Security (Enterprise or Complete)	Symantec Endpoint Protection or Symantec Endpoint Security (Enterprise or Complete)	Symantec Endpoint Security (Enterprise or Complete)
Console	Symantec Endpoint Protection Manager You do not enroll a SEPM domain to the cloud server.	- On-premises: Symantec Endpoint Protection Manager. Log on to SEPM. - Cloud: Symantec Endpoint Security. Log on to your Symantec Security cloud account. You enroll a SEPM domain in the cloud. Enrolling a Symantec Endpoint Protection Manager domain into the cloud console	Symantec Endpoint Security (SES) You do not enroll a SEPM domain in the cloud. Log on to your Symantec Security cloud account. Moving directly from an on-premises Symantec Endpoint Protection Manager (SEPM) option to a fully-cloud managed option Getting started with Endpoint Security

*Client software	Symantec Endpoint Protection client Deploy the client installation package from the Symantec Endpoint Protection Manager.	Symantec Endpoint Protection client *The Symantec Endpoint Protection client is the same as the Symantec Agent. For a successful hybrid deployment, use the latest version of SEPM and 14.3 MP1 or later clients. You manage the agents and some policies from SES. You manage the earlier clients from the SEPM.	Symantec Endpoint Protection client, but is called the Symantec Agent in the SES cloud server. You manage the agents completely from the cloud, which bypasses communication with the on-premises SEPM.
When to use this approach?	- Your network includes remote locations, such as an oil rig or an offshore environment - You work in a government environment where the network is very restricted. - You have a lot of clients in a dark network. - You want the same features as an on-premises management server. However, Symantec Endpoint Protection continues to add features.	- You want to upgrade from 14.3 MP1 or later to Symantec Endpoint Security but you want to move slowly to a completely cloud-managed console. - You want more flexibility; you can move fully to the cloud at a later point. - You have clients on devices that use operating systems that the Symantec Endpoint Security does not support.	- You do not want the cost or overhead of installing and managing a management server and database. - You have multiple Symantec enterprise products and want to share management capabilities across a single management console. - You want unified visibility into threats, policies and incidents from multiple Symantec products, which reduces incident response times from days to minutes. - Symantec Endpoint Security has additional features that Symantec Endpoint Protection on-premises does not have. See: Quick reference for Symantec Endpoint Protection-managed versus Symantec Endpoint Security-managed features in SES

NOTE

*The client functions slightly differently if the Symantec Endpoint Protection Manager manages it rather than SES manages it. The Symantec Endpoint Protection Manager controls more options on the client, while Symantec Endpoint Security controls fewer options. The Symantec Endpoint Protection Manager provides more options for the user to configure; the cloud-managed client provides fewer options. However, Symantec adds new features in Symantec Endpoint Security in monthly refreshes.

More information

- [Management options](#)
- [Comparison between an on-premises Symantec Endpoint Protection 14.x and Symantec Endpoint Security Complete](#)

Enrolling a Symantec Endpoint Protection Manager domain with the cloud server (14.3 RU3 or later)

You must first enroll a Symantec Endpoint Protection Manager (SEPM) domain before you can manage clients and policies from the Symantec Enterprise Security (SES) cloud.

Enrollment with the cloud server installs the Symantec Endpoint Protection Manager connector using an .MSI file. The connector communicates between the cloud server and SEPM.

NOTE

Use this procedure if you have: a Symantec Endpoint Security Complete subscription, a version 14.3 RU3 or later management server and clients, and you want to manage Adaptive Protection. If you have the Symantec Endpoint Security Enterprise subscription or if you use 14.3 RU2 and earlier, see: [Enrolling a Symantec Endpoint Protection Manager domain into the cloud server](#). You must also have administrator access to the Symantec Endpoint Protection Manager.

If you already have a Symantec Security Cloud account, you can still use these steps to enroll the domain. However, the wizard does not create a second Symantec Security Cloud account.

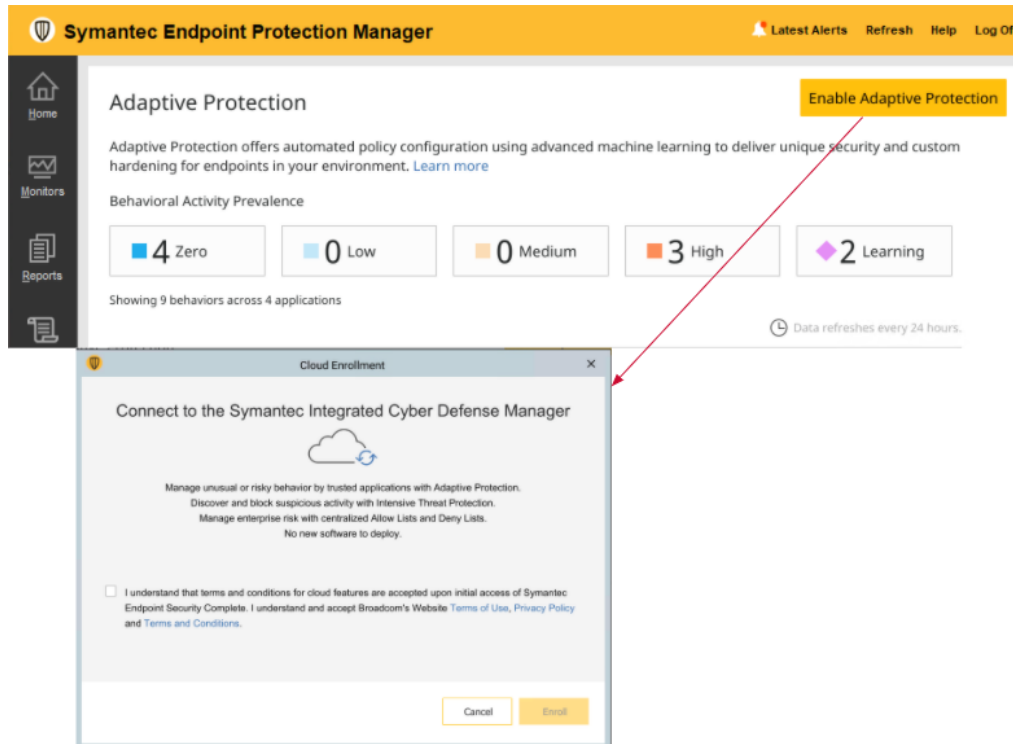
Step 1: Start the enrollment

NOTE

Before you enroll a Symantec Endpoint Protection Manager domain into the cloud, make sure that you install the latest version of Symantec Endpoint Protection Manager.

To start the enrollment from the Symantec Endpoint Protection Manager

1. In Symantec Endpoint Protection Manager, click the **Advanced Security** page.
It can take up to 3 to 4 days before the **Cloud** page changes to the **Advanced Security** page and the Adaptive Protection behavior application heat map appears. During this time, SEPM communicates with and collects data from the SES cloud server. You do not need to enroll the SEPM domain to see the Adaptive Protection heat map. However, if you want to manage the heat map, you must enroll the SEPM domain. You can enroll the SEPM domain immediately or wait to see the populated heat map.
2. On the **Adaptive Protection** page, click **Enable Adaptive Protection**.



3. Agree to the legal agreements and click **Enroll**.
4. In the **Cloud Enrollment** screen, enter your first name, last name, and a valid email address from where you can receive an email message with a PIN number, and then click **Next**.

NOTE

This wizard verifies that this address is the correct address and you are the owner of that email address. You should use the same email address that you use to manage the Symantec Endpoint Protection Manager and that you want to use for your Symantec Security Cloud account.

This step also automatically enrolls the SEPM domain for you.

 Cloud Enrollment ×

Verify Your Email Address



This Symantec Endpoint Protection Manager is enrolled in the cloud console. You must verify the email address you want to use to set up and access your Symantec Security Cloud account. You can use the Symantec Endpoint Protection Manager email address below, or change it. Click **Next** to receive a PIN number that verifies the email address.

If you already have a Symantec Security Cloud account, click **Cancel** and sign on at:
[Symantec Security Cloud](#)

FIRST NAME*

LAST NAME*

WORK EMAIL ADDRESS*

Cancel

Next

You receive an email message at the email address that you specified in the previous step with a 6-digit PIN number. The PIN number is valid for 15 minutes.

8
Lorem Ipsum <sepm_server@companyX.com>



Tue 5/04/2021 10:05 AM

To: You:



Your verification PIN is:

320152

ALERT! DO NOT share this code with anyone. We will never ask you for this code. Verification PIN: 320152 (expires in 3 minutes)

You are receiving this message because you signed up for this alert. Sign on to Symantec Endpoint Protection Manager to modify your notification settings.

Important Information:

If you did not initiate this request, contact your system administrator immediately.



Copyright © 2005-2021 Broadcom. All Rights Reserved.

5. Paste the 6-digit PIN number into the **Enter the PIN to confirm** screen, and then click **Verify**.

 Cloud Enrollment ×

Enter the PIN to confirm



Symantec sent a PIN to the email address **"jsmith@broadcom.com"** for validation. Enter the 6-digit PIN below.

PIN

Didn't receive the PIN? Make sure that you entered the correct work email address. Click **Back** to [Re-enter](#) your email address.

[Resend PIN](#)

Back

Verify

6. After the PIN number is verified and you get a confirmation message, click **Close**.

After the SEPM domain is enrolled:

- The **Enable Adaptive Protection** option changes to **Manage Adaptive Protection**.
- Scroll to the bottom right-hand corner of the heat map and click **Settings**. Under **Enrollment Information**, **Enrollment Status** is set to **Enrolled**.

NOTE

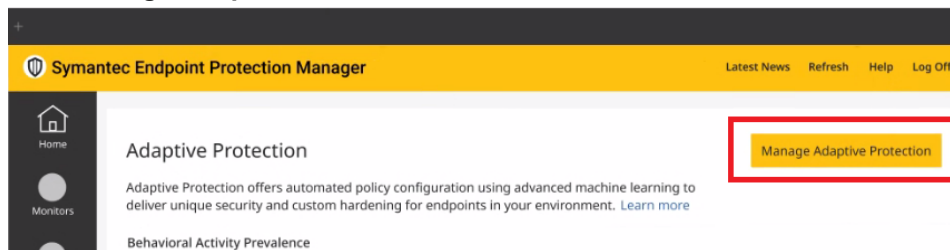
To make sure that the SEPM and the cloud server are connected, scroll down to the bottom right-hand corner of the heat map and see that **Not Connected** changed to **Connected**.

For troubleshooting enrollment issues, see: [Troubleshooting issues on the Advanced Security page](#)

Step 2: Sign on to your Symantec Security Cloud account and create a password

After enrollment, you must sign on to your Symantec Security Cloud account and must create a password. The enrollment and cloud account creation does not automatically create a password for you.

1. Click **Manage Adaptive Protection**.



The Symantec Security Cloud sign on page appears.

[Sign into a Symantec Security Cloud Account](#)

[Getting started with Symantec Endpoint Security](#)

How do I manage clients and policies after I enroll a Symantec Endpoint Protection Manager domain with the cloud server?

After Symantec Endpoint Protection Manager (SEPM) domain enrollment, Symantec Endpoint Protection Manager data gets synced to the Symantec Endpoint Security (SES) cloud server. The data includes the client hierarchy and the policies that the cloud server supports. The sync time is not immediate.

Once the devices and policies are synced, you can manage them from either the Symantec Endpoint Protection Manager or the Symantec Endpoint Security cloud console. This is called hybrid management.

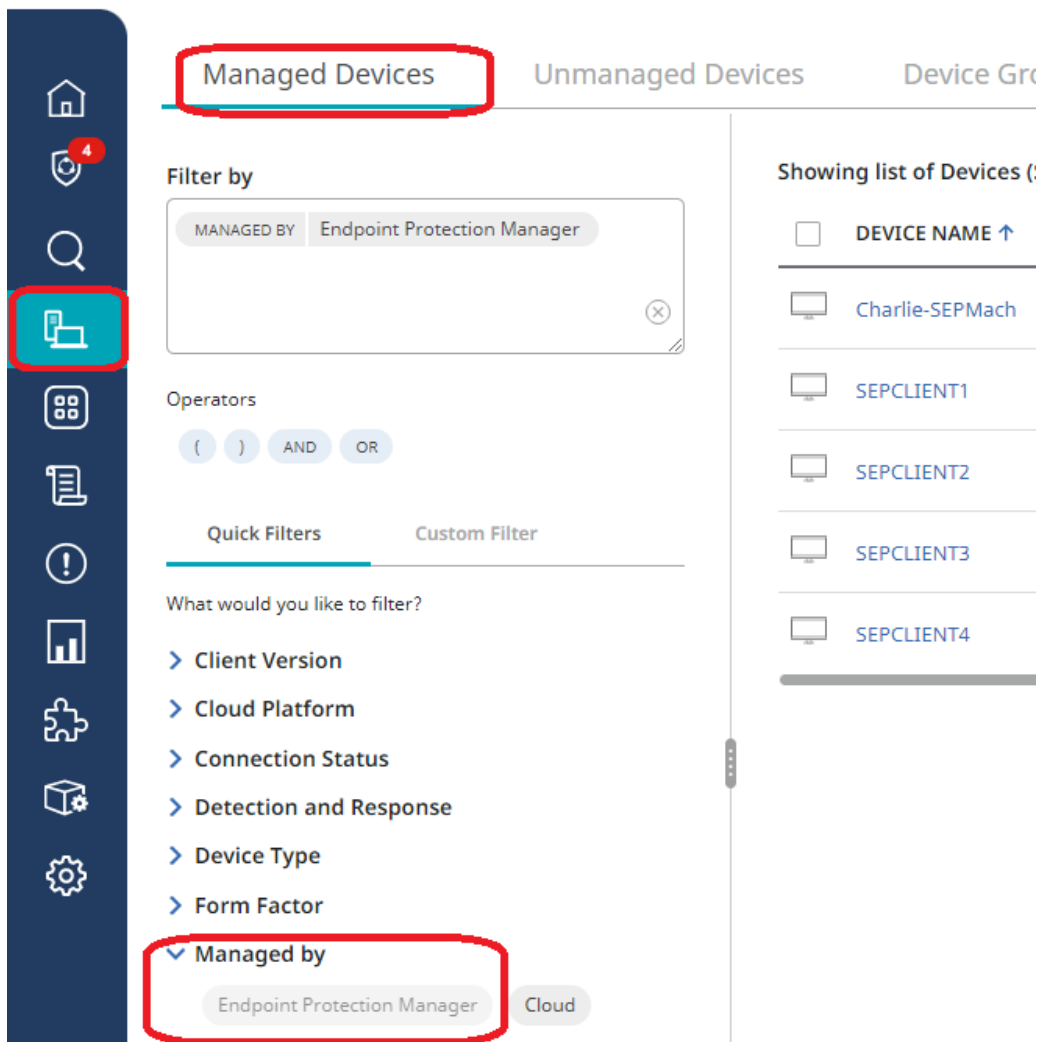
Symantec Endpoint Protection Manager clients are called Symantec Agents in the cloud console.

Step 1: Manage devices from the cloud console

After synchronization, Symantec Endpoint Protection Manager client computers and client groups appear on the SES cloud console automatically as devices.

To view the devices that are synchronized from Symantec Endpoint Protection Manager

1. In the cloud console, on the **Devices** page, do one of the following tasks:
 - On the **Managed Devices** tab, in the **Managed by** drop-down menu, select **Endpoint Protection Manager**. By default, the devices appear in a flat list and not in groups on the **Managed Devices** page.



The screenshot shows the Symantec Endpoint Protection console. On the left sidebar, the 'Devices' icon is highlighted with a red box. The main content area has three tabs: 'Managed Devices' (highlighted with a red box), 'Unmanaged Devices', and 'Device Groups'. Below the 'Managed Devices' tab, there is a 'Filter by' section with a dropdown menu set to 'MANAGED BY Endpoint Protection Manager'. Below this is an 'Operators' section with parentheses and 'AND/OR' buttons. A 'Quick Filters' section is also present, listing various filters like 'Client Version', 'Cloud Platform', 'Connection Status', 'Detection and Response', 'Device Type', 'Form Factor', and 'Managed by' (highlighted with a red box). The 'Managed by' dropdown is currently set to 'Endpoint Protection Manager' with a 'Cloud' option also visible. On the right, a list of devices is shown under the heading 'Showing list of Devices (0)'. The list includes 'Charlie-SEPMach' and 'SEPCCLIENT1' through 'SEPCCLIENT4'.

- On the **Device Groups** tab, go to the **My Company** group.

By default, you manage the organization of your devices in the Symantec Endpoint Protection Manager. You can manage devices in the cloud console only or in Symantec Endpoint Protection Manager only but not both at the same time.

NOTE

If you want Active Directory or some other third-party directory tool to manage your device organization, keep **Manage Devices From the Cloud** turned off.

Whenever you make a change to the device group structure, it takes several minutes before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes. The changes might not take effect.

To manage devices from the cloud console

1. In the cloud console, go to **Integration > Enrollment**.
This setting is disabled by default.
2. Turn on **Manage Devices From the Cloud**.

Step 2: Manage policies from the cloud console

Policies appear in the cloud console automatically on the **Policies** page. You do not need to export your policies from Symantec Endpoint Protection Manager and import them in the cloud, unless you are going to manage your environment completely from SES.

This setting applies to the following bridged policies that are normally present on a Symantec Endpoint Protection Manager normally: the Exceptions policy and the Memory Exploit Mitigation (MEM) policy. This setting keeps SEPM from downsynchronizing these policies and creating new ones in the SEPM.

After domain enrollment, the cloud server always controls the supported policies, which you manage from SES.

You continue to use Symantec Endpoint Protection Manager to manage other policies. Policies are pushed down to Symantec Endpoint Protection Manager, which distributes them to the clients.

To manage policies from the cloud console

1. In the cloud console, go to **Integration > Enrollment**.
This setting is disabled by default
2. Turn on **Manage Policies From the Cloud**.

Step 3: Look for threats that the cloud server detected

On the cloud console, the **Home** page and the **Discovered Items** page provide more comprehensive information about the detections in your environment. Use the **Home** page to check the results of the policy settings and tune the policy settings if necessary.

How a hybrid-managed Symantec Endpoint Protection Manager (SEPM) interacts with the Symantec Endpoint Security (SES) cloud console

Communication and enrollment between the Symantec Endpoint Protection Manager and the cloud server

This section lists some expected behaviors that may occur when you enroll a SEPM domain with the cloud server.

- If the Symantec Endpoint Protection Manager connector cannot obtain the access token to the cloud server, it retries every hour.
- Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud server. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status. See:

[Checking whether the client is connected to the management server and is protected](#)

- The system time for the management server and the Google Cloud Platform (GCP) server must be within 10 minutes of each other. Otherwise, enrollment fails, and you see the following error message:

```
Enrollment in the cloud console cannot complete because the Symantec Endpoint Protection Manager computer date and time does not match the current date and time. Change the setting in the Control Panel, and then retry the enrollment.
```

To resolve the time mismatch, synchronize the Symantec Endpoint Protection Manager server with Network Time Protocol (NTP). See the following for more information:

[NTP: The Network Time Protocol](#)

- You can use the following logs to troubleshoot a failed enrollment: `BRIDGE_INSTALL.log`, `catalinaWs.out`, `Cloud-0.log`, `scm-server-0.log`, and `semapisrv_access_log.date.log`. All of these files are in `\tomcat` \logs, within the Symantec Endpoint Protection Manager installation folder.

Licensing, installation, upgrading, database

- You must purchase a Symantec Endpoint Security license to use or enroll with the cloud server.
- You cannot upgrade a management server from the cloud console.
- You cannot back up or restore the database or Symantec Endpoint Protection Manager settings from the cloud.
- To free up licenses, the Symantec Endpoint Protection Manager database deletes the clients that have not connected to the domain, based on the number of days that you specify. In the cloud server, these clients are automatically deleted after 30 days, and you cannot configure this interval. The clients are deleted first in the Symantec Endpoint Protection Manager database and then in the cloud server. See:

[Purging obsolete clients from the database to make more licenses available](#)

Domain enrollment and unenrollment

When the domain is enrolled:

- Events, policies, clients, and client groups are synchronized.
- Cloud-supported policy features are not available for configuration in Symantec Endpoint Protection Manager.
- Cloud policy settings take precedence.

You can unenroll the default domain if necessary. For example, you might have connectivity issues, or you might decide that you do not want the cloud console to manage your policies. You can unenroll on the enrollment page in Symantec Endpoint Protection Manager or in **Endpoint > Integration > Enrollment** in the cloud console.

The unenrollment process removes the client groups and clients of the unenrolled domain in the cloud. Any associated policies remain in the cloud console as well as related events. See:

- [Enrolling a Symantec Endpoint Protection Manager domain into the cloud server](#)
- [Enrolling a Symantec Endpoint Protection Manager domain into the cloud console \(14.3 RU3 or later\)](#)
- [Unenrolling Symantec Endpoint Protection Manager domains](#)

Sites, replication

- For each site, you enroll one Symantec Endpoint Protection Manager domain per site in the cloud console. You cannot enroll multiple domains even if the domains are in separate sites. You also cannot enroll separate Symantec Endpoint Protection Manager domains if you use the same cloud console account.
- For sites with two Symantec Endpoint Protection Managers that share a SQL Server database and that are configured for failover, you enroll one domain from one of the management servers. The bridge service that communicates between each management server and the cloud console runs on one management server at a time. The service runs on the management server with the higher server priority first. If the first bridge service goes down, the service to the second management server runs instead. You can only manage one domain at a time from the cloud console. The sync between the cloud console and each management server does occur simultaneously.

The following table displays which site configurations the cloud console supports when you enroll a Symantec Endpoint Protection Manager domain.

Table 55: Site configurations that the cloud console supports

Site configuration	Supported on the cloud console
One site, one Symantec Endpoint Protection Manager on one computer with a database on the same computer only	Yes
One site, one Symantec Endpoint Protection Manager on one computer with a Microsoft SQL Server database on the second computer	Yes
One site, multiple Symantec Endpoint Protection Managers	Yes

Site configuration	Supported on the cloud console
Multiple sites, one Symantec Endpoint Protection Manager on each site, with replication*	Yes (14.2 RU1 and later)
Multiple sites, multiple Symantec Endpoint Protection Managers on each site, with replication*	Yes (14.2 RU1 and later)

* Only one Symantec Endpoint Protection Manager on one of the sites in a replication partnership is supported to enroll with the cloud.

For more information, see: [Enrolling sites with replication partners in the cloud server](#)

Groups, clients, locations

- If you rename **My Company** in the cloud console, the group name does not change in Symantec Endpoint Protection Manager.
- Cloud-managed features require a managed client. You cannot manage an unmanaged client or apply a policy that uses cloud features to an unmanaged client. If you apply policies that use cloud features to an unmanaged client, the policy defaults to the equivalent legacy Symantec Endpoint Protection options.
- Version 14 MP2 and earlier client computers appear in the cloud console, but do not support any of the new cloud-based features.
- If the **Manage Devices from the Cloud** option is turned on in the cloud console, the cloud console manages the devices. If it is off, then Symantec Endpoint Protection Manager manages the devices.
If you use Active Directory with Symantec Endpoint Protection Manager to manage groups and clients, then Symantec Endpoint Protection Manager automatically manages devices. In this case, you cannot switch **Manage Devices from the Cloud** to the cloud console. This setting returns control of the device organization only to Symantec Endpoint Protection Manager. It does not affect policy protection on any group. You continue to manage advanced policy features from the cloud console.
- Whenever you make a change to the device group structure, there is several minutes delay before the change appears in Symantec Endpoint Protection Manager. The reverse is also true. The behavior is similar to how Symantec Endpoint Protection Manager replication functions. During the delay, you should not try to make additional topology changes.
- If you add a group or policy in the cloud console that contains any of the following special characters: / \ * ? < > | : " , these characters are converted to a dash in the Symantec Endpoint Protection Manager. For example, if you name a group `Europe***`, on Symantec Endpoint Protection Manager, this group is labeled as `Europe---`.
- The cloud console supports location awareness for 14.3 and later agents, called *policy targeting*. For earlier agent versions, if a Symantec Endpoint Protection Manager group has multiple locations and each location uses a different policy (shared or non-shared), then only the default location's policy gets synched up and applied to the equivalent group on the cloud console. After the cloud console syncs back with Symantec Endpoint Protection Manager, that group's policy in the cloud console is applied as a shared policy to all the locations in the equivalent group on the Symantec Endpoint Protection Manager. This process applies to both the Memory Exploit Mitigation policy and the Exceptions policy in the Symantec Endpoint Protection Manager.
- The cloud console does not support a connection over IPv6. Enrollment of Symantec Endpoint Protection Manager over an IPv6 network results in the following error:

```
An error has occurred requesting the status for this enrollment token.
```

```
Symantec Endpoint Protection Manager cannot connect to the cloud console. Check the network connection and try again.
```

Policies

- You can manage policies from the cloud.
You must still manage policy settings for clients earlier than 14 directly from Symantec Endpoint Protection Manager. However, there are exceptions. If you apply an Exceptions policy from the cloud, and the client supports the exception

type, then the exception applies to the client regardless of version. Memory Exploit Mitigation policies apply to all version 14 clients and later.

- In the Virus and Spyware Protection policy, a cloud icon appears next to some options when the domain is enrolled in the cloud console. If an Intensive Protection policy is in effect, the policy overrides these options.
- The first default cloud policies that you create and assign in the cloud console is appended with a `v` and a number (#) in Symantec Endpoint Protection Manager, as follows: `Default MEM Policy v1`. If you then unenroll and then reenroll the Symantec Endpoint Protection Manager domain, an additional `v#` is appended to the policy name. For example, `Default MEM Policy v1` may become `Default MEM Policy v1 v1` or `Default MEM Policy v1 v3`.
- In Symantec Endpoint Protection Manager, some cloud policies appear in the list on the **Clients > Policies** tab. A cloud icon indicates that the policy originates from the cloud.

Table 56: Cloud icons

Icon	Description
	The group does not inherit the policy from its parent in the cloud console. The policy applies directly to the group.
	The group inherits the policy from its parent in the cloud console.

Some cloud console policies are new policies and some are cloud versions of existing policies. The client version determines which policies the client supports. If you apply a policy to a client that does not support the policy, the client ignores the policy. This behavior is true whether the policy originates in the cloud console or in Symantec Endpoint Protection Manager. The user interface in Symantec Endpoint Protection Manager indicates which options or entire policies the cloud console controls.

- The hybrid-managed cloud console currently supports Symantec Endpoint Protection Manager policies for Windows clients but not for Mac or Linux clients. You must still manage Mac and Linux clients entirely from the cloud or entirely from Symantec Endpoint Protection Manager. See:

[Differences in features between an on-premises SEPM and a cloud-enrolled SEPM](#)

Policy inheritance

Policies that come from the cloud do not follow the policy inheritance configuration for Symantec Endpoint Protection Manager. Instead, they follow the inheritance rules that are defined in the cloud.

Child device groups inherit policies from their parent device group. However, you can apply policies directly to child groups or child devices. You do not have to turn off inheritance. See:

[Differences in features between an on-premises SEPM and a cloud-enrolled SEPM](#)

Differences in features between an on-premises SEPM and a cloud-enrolled SEPM

You manage some policies in the Symantec Endpoint Security (SES) cloud console and the rest in the Symantec Endpoint Protection Manager (SEPM) when your Symantec Endpoint Protection Manager domain is enrolled.

Table 57: Feature reference

Symantec Endpoint Protection Manager	Symantec Endpoint Security
Home page	Home page - Provides a guided first-time user experience to get you familiar with SES cloud features. - Includes a Key Performance Indicator (KPI) bar as well as interactive widgets (charts) with drill-down detail. - Shows detailed visibility into suspicious file detections.
Clients, client groups Managed from the Symantec Endpoint Protection Manager by default.	Devices, device groups To manage groups from the cloud, select the Integration > Enrollment > Manage Devices from the Cloud option. This option affects group creation or deletion and device move or deletion only. The feature works similarly to how Active Directory works with Symantec Endpoint Protection Manager. When the device management option (Manage Devices from the Cloud) for the domain is enabled, you must use the cloud console to organize clients and client groups. If you use the Symantec Endpoint Protection Manager, Active Directory, or you use third-party APIs to manage your devices, you should disable this option. You can view your devices and device groups in the cloud console. You cannot create a group in Symantec Endpoint Protection Manager when its domain is enrolled with the cloud server and the device management option is enabled. When the device management option is enabled, the group structure is managed in the cloud. For information on how the Manage Devices from the Cloud option works, see: Symantec Endpoint Protection Manager enrollment settings
No corresponding configuration.	Policy group
Policy inheritance In Symantec Endpoint Protection Manager, you must disable policy inheritance if you want to directly apply a policy to a child group. Note: If you unenroll the domain, any MEM policies that you directly applied to child groups from the cloud are applied to the child groups and their locations regardless of Symantec Endpoint Protection Manager inheritance settings.	Policy inheritance In the cloud console, policy inheritance is always enabled. However, you can always directly apply policies to child groups to override the parent policy.
Monitor and Reports pages	Incidents and Alerts page You can filter incidents and alerts. Both views provide drill-downs that include enhanced details. A default alert rule notifies the administrator when a specific alert is triggered. Role management provides a way to define which administrators receive alerts about relevant events. You can view and edit predefined alert rules on the Incidents and Alerts > Alert Rules tab. Incidents help you analyze events quickly to make decisions about how to tune policies in your environment. You can view incidents on the Incidents and Alerts > Incidents tab

Symantec Endpoint Protection Manager	Symantec Endpoint Security
Administrator roles • System administrator • Administrator (domain-based) • Limited administrator (policy based) Cloud console administrators and Symantec Endpoint Protection Manager administrators are not linked in any way.	Administrator roles • Super Administrator • Domain Administrator • Limited Administrator • Security Analyst • Viewer Default administrator roles in the cloud console
Console timeout The default is one hour. You can change the timeout.	Console timeout You cannot change the timeout period. The timeout is 2 hours.
Heartbeat option	Not available. All policy changes happen in real time.

The following table displays which policies are available for a Symantec Endpoint Protection Manager enrolled in the cloud, as well as the minimum client version that supports each policy.

Table 58: Policy feature reference

Symantec Endpoint Protection Manager	Symantec Endpoint Security
Out-of-box policies The following policies continue to be managed in Symantec Endpoint Protection Manager: • Firewall policy • Device Control • Intrusion Prevention policy • LiveUpdate policy • Host Integrity policy • Virus and Spyware Protection policy options other than Bloodhound, SONAR heuristics, Download Insight, and scan actions. • Application and Device Control • System Lockdown	Managed from the Symantec Endpoint Protection Manager by default. To manage the following policies from the cloud, select the Integration > Enrollment > Manage Policies from the Cloud option: • Intensive Protection policy • System policy (low-bandwidth option only) • Allow List policy • Deny List policy • MEM policy For information on how the Manage Policies from the Cloud option works, see: Symantec Endpoint Protection Manager enrollment settings The fully cloud-managed Symantec Endpoint Security manages additional policies that Symantec Endpoint Protection does not manage. See: Feature comparison between on-premises products and SES
Download Insight, Bloodhound and Behavioral Analysis (SONAR) settings in Virus and Spyware Protection policy The following settings are not applicable to Symantec Endpoint Protection clients when the domain is enrolled with the cloud server: • Virus and Spyware Protection policy detection actions • Bloodhound settings • Download Insight sensitivity slider • Download Insight prevalence, first-seen, and intranet options • SONAR heuristic detection and SONAR suspicious behavior settings These settings are still used for clients if you unenroll the domain. Note: The default Intensive Protection blocking level is less aggressive than the most aggressive Bloodhound setting in a Virus and Spyware Protection policy. If your current policies specify Bloodhound at its highest level, you might need to increase the Intensive Protection level.	Intensive Protection policy Automatically applied to Windows clients after domain enrollment Replaces some settings in Virus and Spyware Protection policies for Windows clients. These clients use the Intensive Protection policy to replace certain existing settings in the Virus and Spyware Protection policy: • Bloodhound • SONAR heuristics • Download Insight options • Scan actions However, clients still use their Virus and Spyware Protection policy for other options.
Exceptions policy In Symantec Endpoint Protection Manager, there is a single Exceptions policy, which contains exclusions for many different items as well as exclusions for applications. The cloud server Allow List and Deny List policies appear as separate policies in Symantec Endpoint Protection Manager. Items from the cloud server appear in the Exceptions policy > Exceptions list. When the domain is enrolled, you can only create exceptions for the types that are not supported in the cloud server.	Allow List policy Any Allow List policy that you create in the cloud appears in Symantec Endpoint Protection Manager even if you unenroll the domain. The cloud console includes a central list of items that are allowed or blocked so you can view all of these items in one place. The Allow List policy was renamed from the Whitelist policy in 14.3 RU1.

Symantec Endpoint Protection Manager	Symantec Endpoint Security
Exceptions policy Deny List policies from the cloud console are not scan exceptions. However, denied items from the cloud console appear in the Exceptions list.	Deny List policy Any Deny List policy that you create the cloud appears in Symantec Endpoint Protection Manager even if you unenroll the domain. You can configure exceptions in Symantec Endpoint Protection Manager or in the cloud server. The cloud server currently does not support the full range of exceptions. Note: The Deny List policy is a type of application control that uses behavioral analysis (SONAR) in Symantec Endpoint Protection Manager to enforce its rules. It does not use the application control driver in Symantec Endpoint Protection Manager. The Deny List policy was renamed from the Blacklist policy in 14.3 RU1.
No corresponding option. Symantec Endpoint Protection Manager shows low-bandwidth status. You can see whether or not the low-bandwidth option is enabled in External Communications > Cloud Settings . Symantec Endpoint Protection Manager also manages the LiveUpdate AML content that is required for low bandwidth to work.	System policy (low-bandwidth option) The System policy is a new policy in the cloud with no corresponding configuration in Symantec Endpoint Protection Manager. However, the low-bandwidth option requires low-bandwidth Advanced Machine Learning (AML) LiveUpdate content to be available on Symantec Endpoint Protection Manager for the policy to work. Default is off.
Memory Exploit Mitigation (MEM) policy When your domain is enrolled, you must use the cloud server to configure this policy.	Exploit Mitigation policy (MEM) policy 14.2 RU1 and later for custom applications. You must have Application Isolation enabled. The client must have Application Hardening installed. The policy options are comparable to the options in Symantec Endpoint Protection Manager.

Troubleshooting communication issues between a hybrid Symantec Endpoint Protection Manager, clients, and the cloud server

Read about the possible communication issues between Symantec Endpoint Protection Manager (SEPM) and the Symantec Endpoint Security (SES) cloud server in a hybrid environment.

How does the on-premises Symantec Endpoint Protection Manager communicate with the cloud server?

As part of the on-premises SEPM enrollment process, the SEPM uses a connector to connect to the cloud server. The SEPM automatically installs the connector and uploader services, but these services are active only on a SEPM that is enrolled into the cloud. The connector uses the Google Cloud Platform (GCP) to upload group and events data to the cloud.

After the enrolled site synchronizes with the cloud server, the SEPM:

- Uploads the groups, devices, and log events for all clients that are in this site. The on-premises SEPM group structure is one of the first pieces of data that the SEPM sends to the cloud server. Synchronized clients are placed into a duplicate **My Company** group in the cloud.
- Synchronizes reporting events with the cloud server.
- Receives the policies, logs, and commands from the cloud server and immediately passes the data to the clients that communicate with this site.

If a site has multiple management servers, the first enrolled SEPM (SEPM A) uploads the group data. If SEPM A cannot communicate with the cloud server, SEPM B starts to upload group data. SEPM B is based on the management server list.

Troubleshooting communication issues

Issue	Solution
During a management server upgrade, the bridge service stops and fails to sync with the cloud.	Make sure that all management servers in the site have access to the required URLs. As a best practice, allow the following services for connectivity. See: External URLs required for Endpoint Protection (SEP) and Endpoint Protection (SES) • Symantec Cloud API gateway • Cloud notification service (SPOC) • Cloud storage services • SSL/TLS certificates: – http://crl3.digicert.com/DigiCertGlobalCAG2.crl – http://crl4.digicert.com/DigiCertGlobalCAG2.crl – http://ocsp.digicert.com
Synchronization between the Symantec Endpoint Protection Manager and the cloud server is delayed. To verify the delay, the following entry in the <code>semapi_srv_log</code> appears: <pre>[HubSyncCheckTask] ERROR c.s.s.s.m.c.cloud.epmp.HubSyncCheckTask - hub agent [ASSET_UPLOADER] delayed by 1641 hours</pre>	This error occurs in the following situations: • Symantec Endpoint Protection Manager has connectivity to the Internet only sporadically or for a short time during the day. • Your environment uses a proxy setting that is required to access the required URLs. If your environment uses a proxy configuration, it may apply to the logged-in users and not the System user, which Symantec Endpoint Protection Manager runs under. Therefore, Symantec Endpoint Protection Manager cannot connect. To solve this issue: • Check that your firewall and/or proxy settings are not blocking access from the Symantec Endpoint Protection Manager. • Make sure that the Symantec Endpoint Protection Manager can connect to the following URLs: http://crl3.digicert.com/, http://crl4.digicert.com/, and http://ocsp.digicert.com/ Integrating browser extensions with Symantec Endpoint Protection (SEP) to protect against malicious websites • Make sure that your proxy settings apply to the SYSTEM account.
You want to use notifications to tell you whether the management server is synchronized with the cloud.	If the Symantec Endpoint Protection bridge service and uploader services are stopped, the client and the group structure are not synced with the cloud. In 14.3 RU6 or later, the System log > Server Activity log type displays an event that details whether the SEPM enrolled into the cloud server successfully. In addition, SEPM validates several URLs that are required to properly connect with the cloud service (14.3 RU6 and later). SES displays the following alert rule you when the cloud server has not received any data from the SEPM connector for at least 7 days: No recent activity from the SEPM bridge service
After a Symantec Endpoint Protection Manager upgrade, the SEPM does not connect to the cloud server. In the SES cloud log, you see the following 403 error: <pre>Enrollment response code: 403 Failed with error code: 403, not going to retry</pre>	This error occurs if you unenrolled SEPM from the cloud server, which sometimes causes the cloud server to get out of sync. The cloud server may incorrectly communicate that SEPM is still enrolled. To solve this issue, re-enroll the SEPM domain. 1. In the SEPM console, click the Settings option at the bottom of the Advanced Security page. 2. Copy and paste the enrollment token that you obtained from the cloud console Integration > Enrollment page. 3. Click Enroll Symantec Endpoint Protection Manager and confirm whether you want to enroll. SEPM then detects that the cloud server is out of sync.

Issue	Solution
The SEPM is enrolled in the cloud but has synchronization issues.	As of RU7, the Server Activity log type displays whether the SEPM and the cloud server synchronize successfully. These messages include the following situations: <i>Symantec Endpoint Protection Manager failed to synchronize with the cloud.</i> <i>Symantec Endpoint Protection Manager synchronization status with the cloud is unknown.</i> <i>Symantec Endpoint Protection Manager has not synchronized with the cloud.</i>
After enrollment and synchronization with the cloud, you added a client to the SEPM, but the client did not move to the cloud.	Whenever you change the device group structure, there may be several minutes delay before the change appears in the SEPM. The reverse is also true. "Whenever you change the device group structure, there may be several minutes delay before the change appears in the SEPM. During the delay, you should not try to make more topology changes. The changes might not take effect.

More information

- For more information on troubleshooting enrollment issues in SEPM, see: [Troubleshooting issues on the Advanced Security page](#)
- [Enrolling sites with replication partners in the cloud console](#)
- [What happens after you enroll a Symantec Endpoint Protection Manager domain into the cloud console?](#)

Enabling Adaptive Protection in Symantec Endpoint Protection

Learn what the Adaptive Protection feature is and how to enable it from the Symantec Endpoint Protection Manager.

What is Adaptive Protection?

Adaptive Protection protects enterprise environments from the shift in the threat landscape toward sophisticated and targeted attacks. Attackers no longer use general-purpose attack tools. Attackers customize attacks based on tools that exist in the enterprise environment itself. These Living off the Land (LOTL) techniques help attackers move across an environment and evade security providers. To protect an enterprise against targeted attacks, Adaptive Protection uses a rich behavioral analysis engine as well as the global threat telemetry and expertise to:

- Identify the behaviors of trusted applications that have been used as part of an attack chain.
- Profile the normal behavior of trusted applications and processes in the enterprise environment.
- Analyze prevalence to get visibility into the potential impact of eliminating specific behaviors in the environment.

You can use the prevalence analysis that is coupled with correlated MITRE techniques to help determine what application behaviors can be blocked. Any behaviors that are not used or seldom used can be safely blocked. Based on the latest attack trends, Symantec continuously adds behaviors that you can manage with Adaptive Protection.

For more information about Adaptive Protection, see:

[How Symantec Adaptive Protection Marks a New Chapter in Security Defense](#)

Video: [Symantec Endpoint Security Complete \(featuring Adaptive Protection\)](#)

You can [view this custom protection](#) using the on-premises Symantec Endpoint Protection Manager (SEPM). Or you can fine-tune the protection by managing the Adaptive Protection from the Symantec Endpoint Security (SES) cloud console.

Adaptive Protection requirements

To view or manage Adaptive Protection, you must have:

-
- A Symantec Endpoint Security Complete subscription.
 - Version 14.3 RU3 or later Windows clients.
 - The latest version of the Symantec Endpoint Protection Manager.
 - Telemetry enabled for the client groups.

In the Symantec Endpoint Protection Manager, make sure that **Send anonymous data to Symantec to receive enhanced threat protection intelligence** option is enabled. See:

[Managing the pseudonymous or non-pseudonymous data that clients send to Symantec](#)

To view the Adaptive Protection heat map or receive Cloud Analytics notifications, the management server must first complete *light enrollment* with the cloud server.

To manage the Adaptive Protection heat map, you must [fully enroll](#) the management server with the Symantec Endpoint Security cloud server.

How does light enrollment work?

Light enrollment is a background process that occurs as soon as LiveUpdates downloads Adaptive Protection content to Symantec Endpoint Protection Manager for the first time. The purpose of light enrollment is for Symantec Endpoint Protection Manager to establish a method of communicating and receiving data from the Symantec Endpoint Security cloud server. Light enrollment also matches your Symantec Endpoint Security Complete license with the data from your company.

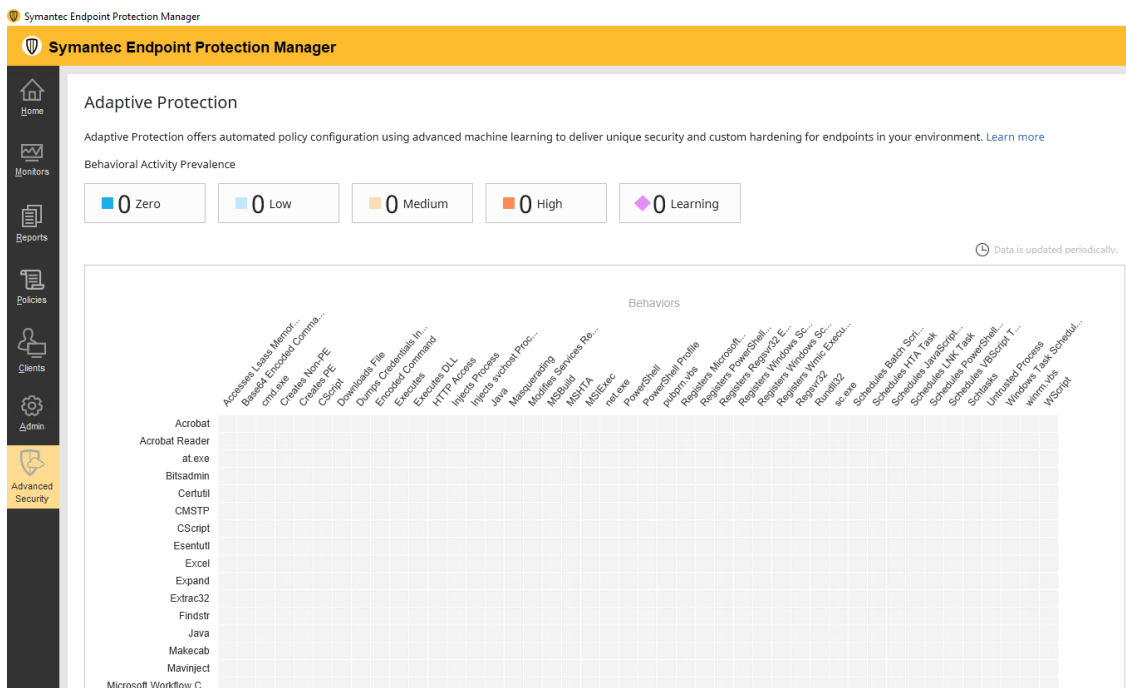
Light enrollment works as follows:

- LiveUpdate downloads content to the Symantec Endpoint Protection Manager, which starts a registration task with the cloud server. This registration task:
 - Validates the Symantec Endpoint Security Complete license.
 - Checks whether the client groups in the SEPM domain have telemetry enabled. If a majority of the clients device hardware keys (MIDs) match, the appropriate API returns a response to the cloud server that indicates that your organization is eligible for enrollment.
- The cloud server authorizes the registration.

If the registration fails, the **Advanced Security** page shows an 401 error. If the SEPM domain is already registered, you see an 403 error. See:

[Troubleshooting issues on the Advanced Security page](#)

The **Advanced Security** page replaces the **Cloud** page. The Adaptive Protection page shows an empty heat map for up to 3 or 4 days until Symantec learns enough about the behaviors in your environment, and SEPM communicates with the cloud server.

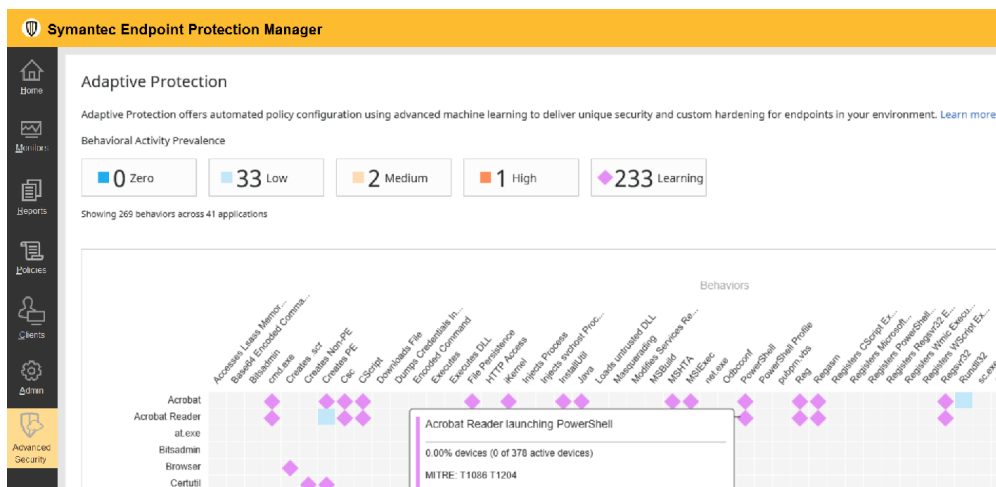


NOTE

If you have a Symantec Endpoint Security Enterprise subscription, you continue to see the **Cloud** page.

Understanding the Adaptive Protection heat map

The Adaptive Protection page shows a heat map widget that uses the color coding to show the prevalence of trusted application behaviors in your environment. Heat map data is collected from all devices that use a particular Adaptive Protection policy. The data in the heat map is based on telemetry that is collected from devices in the past 90 days.



The following icons in the heat map show the prevalence of the application behavior pairs.

- **Zero prevalence**
This application behavior is not prevalent. No devices would be affected by a change in the policy action.
- **Low prevalence**

This application behavior is not prevalent. Few of your devices would be affected by a change in the policy action.

- **Medium prevalence**

This application behavior is somewhat prevalent. Some of your devices would be affected by a change in the policy action.

- **High prevalence**

This application behavior is very prevalent. If you change the policy action for this application behavior, you affect up to 80 percent of your devices.

- **Learning**

Adaptive Protection is still learning about this application behavior and does not have enough current data to assign a prevalence value. This may also occur if up to 5% of your devices are new. For example, your organization may replace laptops with new images frequently. Adaptive Protection assigns a prevalence after it observes the application behavior for 90 days.

Initially, all application behaviors are set to **Learning** with an action of Monitor.

Managing the Adaptive Protection policy in the cloud

If you want to adjust Adaptive Protection for your environment, you must switch your management from the on-premises management only to the hybrid management. Hybrid management lets you manage your clients from either the on-premises Symantec Endpoint Protection Manager or the SES cloud console. However, you manage Adaptive Protection policies from the cloud console and not the Symantec Endpoint Protection Manager. For hybrid management, enroll the Symantec Endpoint Protection Manager domain in the cloud server.

Step	Description
Step 1: Enroll the Symantec Endpoint Protection Manager domain in the cloud server.	• For 14.3 RU3 with a Symantec Endpoint Security Complete license, see: Enrolling a Symantec Endpoint Protection Manager domain with the cloud server (14.3 RU3 or later) • For 14.3 RU2 and earlier or with a Symantec Endpoint Security Enterprise license, log on to your Symantec Security Cloud, obtain a token, and paste the token in the Symantec Endpoint Protection Manager. See: Enrolling a Symantec Endpoint Protection Manager domain into the cloud server
Step 2: In the cloud console, create an Adaptive Protection policy.	In the Symantec Endpoint Security cloud console, create an Adaptive Protection policy and apply the policy to the Symantec Endpoint Protection Manager-managed devices. For more information on how to use the Adaptive Protection feature in the cloud console, see: Using Adaptive Protection

NOTE

If you manage Adaptive Protection from the cloud console and do not want to refresh the application behavior heat map in Symantec Endpoint Protection Manager, go to **Settings** and turn off **Adaptive Protection**.

Viewing Cloud Analytics incidents on Symantec Endpoint Protection Manager (14.3 RU8 and later)

Symantec Endpoint Protection enhances your incident detections with data that the cloud-based Cloud Analytics service gathers.

What are Cloud Analytics?

Cloud Analytics delivers post-infiltration breach detection capabilities. These capabilities help you discover and act on sophisticated, targeted, and human-driven attacks that are currently occurring within your environment. Cloud Analytics focuses on discovering attacks that other deployed security products can miss.

The Cloud Analytics service combines the research from the Symantec Threat Hunter team to find known and unknown attacks before they attack your environment. The analytics evolve to match with new attack patterns. Symantec analyzes the data from known compromised machines at the process and file level, and assesses the standard tools that are used at the time of compromise as well as the network activity. This telemetry is fed into the learning model to train it on how a targeted attack behaves. When Symantec sees similar suspicious behavior, the incidents are sent directly to the Symantec Endpoint Protection Manager. A notification displays a detailed analysis of the attacker, techniques, impacted machines, and remediation guidance.

Cloud Analytics is the same technology as Targeted Attack Analytics that Symantec EDR provides.

NOTE

Cloud Analytics is part of Adaptive Protection.

Viewing Cloud Analytics notifications

When the Cloud Analytics service detects an incident, the incident passes from through the Symantec Endpoint Security cloud server and displays a notification for the events in the incident in the Symantec Endpoint Protection Manager.

See: [Understanding incidents, events, and entities](#)

The Cloud Analytics service continually reevaluates events that it may have seen before based on new information. The cloud can determine activity that was previously suspicious as no longer suspicious. For example, you may see the following event: Updated - Not Suspicious DGA Beacons.

You might see an average of 10-15 events per incident. The management server does not usually display events for behaviors that the Symantec Endpoint Protection client blocks.

To receive these notifications, you must follow the same requirements as the [Adaptive Protection heat map](#). After you log on to Symantec Endpoint Protection Manager using a Symantec Endpoint Security Complete license, [light enrollment](#) starts. Light enrollment can take up to 24 hours. Symantec Endpoint Protection Manager then displays the incidents that the Cloud Analytics service detected.

NOTE

You do not need to fully enroll Symantec Endpoint Protection Manager with the cloud server.

To view Cloud Analytics events

1. In the console, click **Monitors** page > **Notifications**.
2. On the **Notifications** tab, click **Advanced Settings**, and the **Notification name** drop-down list.
3. In the **Select Notification Name** dialog box, select **Cloud Analytics Breach Detection**, and click **OK**.

Symantec Endpoint Protection Manager

Latest Alerts Refresh Help Log Off

Summary Logs **Command Status** Notifications

Notifications

Tell me more... Auto-refresh: Every 30 seconds

Last updated: 08/08/2023 08:38:45

Notification Conditions

☐ Acknowledge all notifications in this filtered list
[Details](#)

Ack	Report	Time	Created By	Subject	Message
☐		08/07/2023 22:34:05	admin	LOW: TAA EICAR	Targeted Attack Analytics test
☐		08/07/2023 21:40:08	admin	HIGH: Suspected Breach	BITS Jobs; PowerShell; Security Account Manager
☐		08/07/2023 21:37:05	admin	MEDIUM: DGA Beacons	Domain Generation Algorithm usage detected
☐		08/07/2023 21:37:05	admin	Updated - Not Suspicious: DGA Beacons	Symantec has determined that this incident is not suspicious activity.
☐		08/07/2023 21:34:32	admin	Updated - Not Suspicious: TAA EICAR 2	Symantec has determined that this incident is not suspicious activity.
☐		08/07/2023 21:34:32	admin	LOW: TAA EICAR 2	Suspicious Behavior adversary: DemoActor; Credential Dumping (SAM); Data Compressed

To view Cloud Analytics submissions

You can view the incidents that Symantec Endpoint Protection Manager submits to the Symantec Security Response team for review. Also, you can use the report to investigate the activity for a particular client computer. You do not configure the actions that the client takes on an event.

1. In the console, click **Monitors > Logs**.
2. On the **Logs** tab, select the **System** log type and click **Client Activity**.
3. Click **View Log**.

Turning off Cloud Analytics notifications

If you do not want to view the notifications that Cloud Analytics generates in the Symantec Endpoint Protection Manager > **Monitors > Notifications** tab, you can turn the notifications off.

NOTE

Symantec recommends that you keep the Cloud Analytics data refresh turned on.

To disable the Cloud Analytics notifications

- Stop all Symantec Endpoint Protection Manager services:
 - Symantec Endpoint Protection Manager
 - Symantec Endpoint Protection Manager API Service
 - Symantec Endpoint Protection Manager Webserver

[Stopping and starting the management server service](#)

[Stopping and starting the Apache Web server](#)

- Go to: <SEPM_Install>tomcat\etc

Where *SEPM_Install* represents the installation folder for Symantec Endpoint Protection Manager.

- Open the `conf.properties` file, add the following new line at the end, and save the file:
`scm.targeted.attack.analytics.feature.enabled=false`
- Restart all Symantec Endpoint Protection Manager services.

Refreshing Cloud Analytics data

By default, Symantec Endpoint Protection Manager refreshes the Cloud Analytics data every 24 through 48 hours. If your environment has low bandwidth, you may want to disable the ability to refresh the data. You can enable or disable this option only if you [fully enroll](#) Symantec Endpoint Protection Manager in the cloud.

To enable or disable the Cloud Analytics data refresh

- In the Symantec Endpoint Protection Manager, go to **Settings** and turn off **Enable Cloud Analytics**.

Troubleshooting issues on the Advanced Security page

Learn how to troubleshoot problems when you try to activate Adaptive Protection on the **Advanced Security** page.

These issues apply to Symantec Endpoint Protection 14.3 RU3 and later.

Activating Adaptive Protection

When you try to enroll the Symantec Endpoint Protection Manager domain into the cloud and activate Adaptive Protection on the **Adaptive Security** page, you may see the following message: Symantec Endpoint Protection Manager encountered an error while activating Adaptive Protection.

The following table displays the possible causes and the solutions.

Cause	Solution
Licensing: • You are using an out-of-date license. • You may have an on-premises Symantec Endpoint Protection only license. You need a Symantec Endpoint Security Enterprise or a Symantec Endpoint Security Complete license to enroll with the cloud server.	Contact your partner or distributor to renew or upgrade your license to new Symantec Endpoint Security Complete or Symantec Endpoint Security Enterprise subscription. More information: Purchasing and renewing subscriptions in Symantec Endpoint Security Licensing FAQs for Symantec Endpoint Security
The management server is not collecting telemetry from your clients: 1. You may get submissions for some of your clients, but not from all the clients in all the groups. 2. Clients may not be communicating with all Symantec components. 3. If you use one or more proxies in your environment to redirect the necessary traffic to the Symantec servers, make sure that your network firewall allows the URLs that Symantec uses to perform multiple functions.	1. Make sure that you enabled client submissions for all your groups, rather than a subset of clients within your groups. See: Managing the pseudonymous or non-pseudonymous data that clients send to Symantec 2. Make sure that the following ports are open: TCP 139, 445, 443; HTTPS 443. See: Communication ports for Symantec Endpoint Protection 3. If you use proxies, allow the following URLs: External URLs required for Endpoint Protection (SEP) and Endpoint Protection (SES)

Symantec Security Cloud account issue: 1. You do not yet have a Symantec Security Cloud account. 2. Someone in your organization already has a Symantec Security Cloud account. For first-time purchases, a new tenant is automatically created. You should not create multiple tenants. The information for the tenant is based on the email that your partner submitted to Broadcom for the contract.	1. You must create a Symantec Security Cloud account manually. To sign in to Symantec Security Cloud, from a web browser go to the following URL: securitycloud.symantec.com See: Sign into a Symantec Security Cloud Account 2. For help with an existing account, open a Global Customer Car (GCA) case using one of the following methods: • Submit a Customer Care webform: https://ca-broadcom.wolkenservicedesk.com/web-form • Chat with a Customer Care representative with the BOT: https://support.broadcom.com/security • Log a case through your Support Online account: http://support.broadcom.com • Call: • North America: 1-800-225-5224. • Other regions: https://support.broadcom.com/contact-support.html
After you select the Enable Adaptive Analysis option, the Advanced Security page displays a 403 error.	This error occurs for the following reason: The cloud server has not been able to authorize the SEPM and therefore cannot provision the tenant on the cloud server. This error occurs infrequently and when you have a Symantec Endpoint Security Enterprise license only. To solve this issue: 1. Enroll the SEPM domain by selecting the Settings option at the bottom of the Advanced Security page. 2. Copy and paste the enrollment token that you obtained from the cloud console Integration > Enrollment page. 3. Click Enroll Symantec Endpoint Protection Manager and confirm whether you want to enroll.

If you are still unable to solve the problem, contact Broadcom Support, see: [Symantec Enterprise Security](#)

Enrollment issues

The following table displays some of the issues and solutions that may occur when you try to enroll the SEPM domain.

Issue	Description
The Symantec Security Cloud Account Not Created message appears. 	This message appears when one of the following situations occurs: • A different Symantec Endpoint Protection Manager domain is already enrolled. You can enroll one domain at a time into the cloud server. To enroll the domain that you want, first unenroll the domain you do not want. Then reenroll with the domain that you do want. To unenroll a domain, on the Settings page, turn off the Enrollment Status toggle. • The wizard did not create a Symantec Security Cloud account because you already have one at the address that you specified in the Verify Your Email Address screen. To work around this issue, directly sign on to your Symantec Security Cloud account. However, the wizard enrolled the SEPM domain for you.

This enrollment token is for a cloud domain that already has an enrolled Symantec Endpoint Protection domain. Continuing with enrollment will merge this site's data into the existing Cloud domain for disaster recovery. If this site is not the same Symantec Endpoint Protection domain, this action may result in unpredictable behavior.	The Symantec Endpoint Protection Manager detected that you already enrolled a domain with the cloud server using the same token. You should not have multiple SEPM installations that are enrolled into one SES domain, or else the data from multiple domains is merged together. - Click Cancel to stop the enrollment and get a different enrollment token. - Click Continue if you are recovering from a backup that was taken before you enrolled.
I want to use a different email address to create my Symantec Security Cloud account than the one I just used.	If you have already created an account using this wizard, you cannot use the wizard again. Instead, sign on to your Symantec Security Cloud account to access SES, and create a system administrator account. For more information, see: Creating an administrator account If someone from your organization has already created an account, you might not be able to sign on.
The data in the heat map has not changed since I last looked.	The Adaptive Protection behavior heat map data refreshes once every 24 hours. Because the heat map does not have a time stamp, you should check the data once a day.

Known issues

Error	Solution
When you click the Advanced Security page, you may see the following error message: The current license is no longer entitled to Adaptive Protection	This issue occurs if you are using a Symantec Endpoint Security Enterprise license to enable Adaptive Protection. You must purchase a Symantec Endpoint Security Complete license from your partner or distributor .
When you click the Advanced Security page, you may see the following error message: sym-ui-sep-shared.errors.ERROR	To work around this issue, try the following tasks in order. After each task, wait for the Adaptive Protection heat map to appear. - In the upper right-hand corner, click Refresh. - Navigate to another page and then back to the Advanced Security page. - Both log out from and close SEPM and then relaunch SEPM. Click the Advanced Security page.

See: [Troubleshooting communication issues between a hybrid Symantec Endpoint Protection Manager, clients, and the cloud server](#)

How does the Symantec Endpoint Protection Manager Exceptions policy interact with the Symantec Endpoint Security (SES) cloud console?

How do Exceptions policies work on the cloud console?

The cloud console does not support all the exceptions that the Symantec Endpoint Protection Manager supports. After you enroll a Symantec Endpoint Protection Manager (SEPM) domain in the cloud server, the original Symantec Endpoint Protection Manager Exceptions policy divides into two policy types in the cloud console, based on the types of exceptions, called the **Deny List policy** and the **Allow List policy**.

The exceptions that the cloud policies do not support remain in the Symantec Endpoint Protection Manager Exceptions policy. After the cloud server and Symantec Endpoint Protection Manager synchronize, the cloud-based policies are imported back into Symantec Endpoint Protection Manager.

For example, assume that in Symantec Endpoint Protection Manager you create a policy that is called *SEPM Exceptions Policy*. This policy includes an Application exception, a Trusted Web Domain exception, and an Application to Monitor exception. After you enroll in the cloud server, the cloud-based exceptions in *SEPM Exceptions Policy* are separated into two policies. These policies are called *Imported SEPM Exceptions Policy (BL)* and *Imported SEPM Exceptions Policy (WL)*. The Deny List policy is created with the Application exception only, and the Allow List policy is created with the Application exception and the Domain exception. The original Symantec Endpoint Protection Manager *SEPM Exceptions Policy* retains the Application to Monitor exception. After the cloud server synchronizes with Symantec Endpoint Protection Manager, the Symantec Endpoint Protection Manager displays three policies that are assigned to the same group: *SEPM Exceptions Policy*, *Imported SEPM Exceptions Policy (DL) v1*, and *Imported SEPM Exceptions Policy (AL) v1*

In the cloud console, the Blacklist policy was renamed to the Allow List policy. The Whitelist policy was renamed to the Allow List policy.

For more information, see:

[Creating exceptions for Virus and Spyware scans](#)

In addition, the cloud console's Allow List and Deny List policies do not support all the actions that the Symantec Endpoint Protection Manager Exceptions policy supports. The Application exception in the cloud console's Allow List policy only supports the **Ignore** action. The Application exception in the cloud console's Deny List policy only supports the **Quarantine** action. If you add an Application exception in the Symantec Endpoint Protection Manager Exceptions policy and then enroll Symantec Endpoint Protection Manager in the cloud server, the actions automatically change in the cloud policies. The **Log only** action is converted to the **Ignore** action for the Allow List policy. The **Terminate** and **Remove** actions are converted to the **Quarantine** action. After these policies are imported back into Symantec Endpoint Protection Manager, the management server keeps the action from the cloud console policies.

For more information, see:

[Monitoring an application to create an exception for the application on Windows clients](#)

Which exceptions are supported and not supported on the cloud console?

The cloud console supports the following exceptions on Windows clients:

Deny List policy:

- Hash (SHA-256)

Allow List policy:

- Certificate
- Filename
- Domain
- Hash
- File path
- Extension
- IPS Host

After you enroll Symantec Endpoint Protection Manager in the cloud server, the Windows exceptions in the Symantec Endpoint Protection Manager Exceptions policy convert to the following policy type and exception type:

Table 59: SEPM Windows exceptions and how they convert to cloud-based exceptions

Symantec Endpoint Protection Manager Exceptions policy	Deny List policy	Allow List policy
Application	Hash (SHA-256 only)	Hash (SHA-256 only)
Certificate	N/A	Certificate
File > Security Risk/SONAR	N/A	Filename
Folder > Security Risk/SONAR	N/A	Path
Trusted Web Domain	N/A	Domain

The following Windows exceptions remain in the Symantec Endpoint Protection Manager Exceptions policy and are not supported in the cloud console:

- Application to Monitor
- Extensions
- File - Application Control
- Folder - Application control
- Known Risks
- Tamper Protection Exception
- DNS or Host File Change Exception

The cloud server does not support Linux client exceptions or Mac client exceptions. All Linux exceptions items and Mac exceptions items remain in the Symantec Endpoint Protection Manager Exceptions policy.

NOTE

You can also add exceptions directly into the cloud console using a .csv file of checksums that you export from Symantec Endpoint Protection Manager. This file fingerprint list contains the path and the file name and corresponding checksum for each executable file or DLL that resides in a specified path on the computer. See:

[Creating a file fingerprint list with checksum.exe](#)

For more information, see:

[Which Windows exceptions do I use for what type of scan?](#)

Exceptions that users can add on the Windows client

The Symantec Endpoint Protection Manager Exceptions policy allows you to enable users on the Windows clients to add exceptions (called client restrictions).

If Symantec Endpoint Protection Manager is enrolled in the cloud server, Symantec Endpoint Protection Manager does not display the following client restrictions:

- Application Exception
- File Exception
- Folder Exceptions > Security risk Exception/SONAR Exception
- Trusted Web Domain Exception
- Certificate Exception

NOTE

In addition, on Windows clients that a cloud-based exceptions policy controls, these exceptions do not appear in the client user interface.

Symantec Endpoint Protection Manager does display the following client restrictions, whether or not Symantec Endpoint Protection Manager is enrolled.

- DNS or Host File Change Exception
- Extension Exception
- Known Risks Exception

For more information, see:

[Restricting the types of exceptions that users can configure on client computers](#)

Issues with enrolling and synchronizing Exceptions policies with the cloud server

- A Deny List policy or Allow List policy gets automatically created in the cloud console only if the original Symantec Endpoint Protection Manager Exceptions policy includes the exceptions that the Deny List policy and the Allow List policy support. Otherwise, the cloud console ignores the Exceptions policy.
- After enrollment, only assigned Symantec Endpoint Protection Manager Exceptions policies synchronize with the cloud server and then get imported back onto Symantec Endpoint Protection Manager. Unassigned policies remain in Symantec Endpoint Protection Manager as non-cloud-based Exceptions policies. Also, if the assigned Symantec Endpoint Protection Manager Exception policy has no Deny List exceptions or Allow List exceptions, then a corresponding empty Deny List policy and/or empty Allow List policy gets created in the cloud console for that group.
- After enrollment, you can create and assign non-cloud-based Exceptions policies in Symantec Endpoint Protection Manager. However, these policies must include Symantec Endpoint Protection Manager-based exceptions only, and not cloud-based exceptions. If you create and assign a cloud-based Deny List policy or Allow List policy, these policies get synchronized and imported into Symantec Endpoint Protection Manager.
- Exceptions policies that you created in the cloud console remain in Symantec Endpoint Protection Manager after you unenroll the domain. But these cloud-based policies get unassigned from a group in Symantec Endpoint Protection Manager. You can merge them, reassign them, or delete them if you no longer need them.
- If you import a Symantec Endpoint Protection Manager Exceptions policy into the cloud console and that policy has application exceptions, the exceptions are lost after import. You must then manually re-add the application exceptions into the cloud console's Deny List and Allow List policies. The cloud console maintains the other types of exceptions, such as the certificate exception.

Enrolling sites with replication partners in the cloud server

How do you enroll a site in the cloud server?

In 14.3 MP1 (14.3.1169.0100) and later, you set up replication between one site that is enrolled in the cloud server, and more sites that are not. You enroll one site as the primary site. All other sites can replicate directly with the primary site, or can replicate with each other. For example, if Site A is the primary site, you enroll Site A into the cloud server. You configure Site B and Site C to replicate with Site A. Or, you can configure Site B to replicate with Site A, and configure Site C to replicate with Site B.

Table 60: Process for enrolling multiple replicated sites

Task	Description
Step 1: Replicate the two sites before you enroll in the cloud server.	Replicate all policies, groups, and log events before you enroll the primary site to avoid any database conflicts. You can also add a replication partner after you enroll the primary site in the cloud. The primary site can have multiple partner sites. See: • Replicating data immediately • What are sites and how does replication work?
Step 2: Enroll the primary site.	Choose and enroll one site as the primary site to perform the enrollment and any further actions, such as creating policies. For sites with multiple management servers, you only enroll one of the management servers. Any additional management servers are enrolled automatically. You do not enroll the second site, or the partner site, in the cloud server
Step 3: Wait for synchronization to occur.	After the enrolled primary site and the cloud server synchronize, the following events occur on the primary site: • The bridge service is installed on all management servers automatically. However, the bridge service is only active on the management server that you used to enroll in the cloud server. • The primary site synchronizes reporting events with the cloud server. • The primary site uploads the groups, devices, policies, log events, client packages, and definitions for all clients that are not connected to this site. • The primary site receives the policies, logs, and commands from the cloud server and immediately passes the data to the clients that communicate with this site. For more information, see: How do I manage clients and policies after I enroll a Symantec Endpoint Protection Manager domain with the cloud server?
Step 4: Replicate the primary site and any partner sites.	Schedule the replication so that both sites have the same enrollment data. After the replication occurs, the following events occur on the partner site: • The partner site receives the content from the cloud server that is based on the replication schedule with the primary site. The clients that are connected to the partner site then receive this data. • The partner site gets the enrollment details from the primary site. These details appear on the Symantec Endpoint Protection Manager Advanced Security page > Settings > Troubleshooting. • The management servers in the partner sites do not install the bridge service. Therefore, the partner site does not synchronize directly with the cloud server. For more information, see: How to install a second site for replication
Step 5: (Optional) Switch control of groups and devices to the cloud server.	By default, when you enroll an unreplicated Symantec Endpoint Protection Manager domain, the cloud server manages the client group structure. By default, when you enroll a replicated site, Symantec Endpoint Protection Manager manages the group structure. • If Symantec Endpoint Protection Manager is the primary, you can add groups and policies on the primary site, which then gets replicated on the partner site. • If you make the cloud server the primary, first run replication with the partner site. This replication ensures that groups and policies you added on the partner site sync to the cloud server. To switch control to the cloud server, enable the Manage Devices from the Cloud option after enrollment in Integration > Enrollment in the Symantec Endpoint Security cloud console.

You cannot perform failover or load balancing for the replicated partner.

See: [Setting up failover and load balancing](#)

NOTE

If you add new clients to the replication partner site after the primary site synchronizes with the cloud server, these clients appear in the **Default** group in the cloud. Instead, wait until the replication site synchronizes with the primary site, and the primary site synchronizes with the cloud server until you add more clients to the new groups.

Removing and restoring replication between the sites that are enrolled in the cloud server

If you remove the partnership between the primary site and a partner site, you also remove the relationship with the cloud server.

To restore the partnership with the primary site, use the **Add Existing Replication Partner** wizard.

You can also enroll the partner site in the cloud server directly as an individual site. In this case, you must create a different Symantec Security Cloud account. To restore the partnership with the primary site, you must unenroll the partner site. Then, on the primary site, reconfigure the partnership with the **Management Server Configuration Wizard**.

NOTE

As a best practice, keep the partner site as an individual site and do not try to restore the replication with the primary site.

For more information, see:

- [Disabling replication and restoring replication before and after an upgrade](#)
- [Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)

Troubleshooting replication for a site in the cloud server

To get information about primary site enrollment and replication:

- Look for replication events.
On the primary site, open the **System log > Administrative** log type, and look for the **Replication events** event type. See:
[Viewing logs](#)
- Look at the enrollment status of the partner site's on the Symantec Endpoint Protection Manager **Advanced Security > Settings** page:
On the partner site, the **Enrollment Status** displays **Enrolled**.
Other fields such as **Connection Status** display **None**.
To display the enrollment information, see **Troubleshooting**.

[How a hybrid-managed Symantec Endpoint Protection Manager \(SEPM\) interacts with the Symantec Endpoint Security \(SES\) cloud console](#)

Updating clients in low-bandwidth environments

What is low-bandwidth mode?

The low-bandwidth mode is an option for those environments that meet at least one of the following criteria:

- Require infrequent virus and spyware, behavioral analysis (SONAR), and IPS content updates
- Have low connectivity to the cloud server

Low-bandwidth clients receive updates infrequently. Symantec updates low-bandwidth content once a week. In low-bandwidth mode, you can use the aggressive mode policy to tune the security on your endpoints even more. See:

[How does Symantec Endpoint Protection use advanced machine learning?](#)

You must be enrolled in the cloud server to use the low bandwidth option. Low bandwidth is off by default.

- In the cloud console, enable low-bandwidth mode in the Default System Policy (14).
- Make sure that LiveUpdate downloads low-bandwidth content.
- Create a client group that gets low-bandwidth content.

After you enable the low-bandwidth mode, you can see its status in the **Clients** tab in the **Default** view and the **Protection Technology** view. You can also generate reports based on low-bandwidth content distribution.

Enable the low-bandwidth mode from the cloud

You enable or disable low-bandwidth mode in the System Policy in the Symantec Endpoint Security (SES) cloud console.

1. In the SES cloud console, go to **Policies > Default System Policy (14)**. You must have a trial version or purchased version of the product.
2. Turn on **Run in low Bandwidth Mode**.
3. Click **Save Policy**.

Download low-bandwidth content to Symantec Endpoint Protection Manager (SEPM)

Advanced Machine Learning content is downloaded and enabled by default. You can use the following procedures to verify that they are enabled.

To download low-bandwidth content to Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager console, click **Admin > Local Site > Edit Site Properties**.
2. Click to select the **LiveUpdate** tab, then click **Change Selection** next to **Content Types to Download**.
3. Make sure the box next to **Advanced Machine Learning** is checked.
4. Click **OK > OK** to save the changes.

To include low-bandwidth content in LiveUpdate Content Policy

In the Symantec Endpoint Protection Manager console, go to **Policies > LiveUpdate**, and then edit the policy that is assigned to the group that contains the low-bandwidth-enabled clients.

1. Click **LiveUpdate Content**, then double-click **LiveUpdate Content Policy**.
2. Under **Windows Settings**, click **Security Definitions**.
3. In the cloud console, click **Devices**, and then add a child group under **My Company**.
4. Ensure that the **Advanced Machine Learning** box is checked.
5. Click **OK** to save the changes.

Creating a group for low-bandwidth clients

1. In the cloud console, click **Devices**, and then add a child group under **My Company**.
If you cannot add a child group, enable **Manage Devices** in the cloud console (**Settings > Symantec Endpoint Protection Manager Enrollment**). Otherwise, add the group in Symantec Endpoint Protection Manager. If you use Active Directory synchronization, add the group through Active Directory.
2. Apply the System Policy to this group that you previously configured for Low Bandwidth. On the device group, click **Apply Policy**, add the System Policy, and then click **Submit**.
3. In the Symantec Endpoint Protection Manager console, ensure that the LiveUpdate Content Policy that you previously configured applies to the group you created. Policy inheritance that you enable or disable in Symantec Endpoint Protection Manager applies only to Symantec Endpoint Protection Manager policies, and not to cloud-based device policies.

You may need to allow some time for the group to sync from the cloud server.

Running reports on the clients that run in low-bandwidth mode

You can run a report to list the clients that receive low-bandwidth content.

1. In the Symantec Endpoint Protection Manager console, click **Reports > Quick Reports**, and then make the following selections:
 - Report type: **Computer Status**
 - Select a report: **Low Bandwidth Content Distribution**
2. Select a time range: **Additional Settings for more options**.
3. Click **Create Report**.

Monitoring roaming Symantec Endpoint Protection clients from the cloud console

Roaming Symantec Endpoint Protection clients are the clients that intermittently connect to the management server. Roaming clients access the Internet at different locations, such as airports, hotels, or at other companies, where they are at higher risk. Symantec Endpoint Protection Manager provides on and off-network protection for these client computers using location awareness.

Roaming clients automatically send critical events to the cloud console when the clients cannot connect to the management server. After the roaming client reconnects to the management server, the clients send any new critical events on the management server. The client is also no longer considered to be roaming.

Use the list of critical events as a way to strengthen the security policies on the Symantec Endpoint Protection Manager. For example, suppose Employee1's client has a higher number of denial-of-service attacks when Employee1 is located in a particular hotel. Therefore, you can create a location for that hotel and enable denial of service detections in the Firewall policy.

For more information, see:

- [What are the critical events that the cloud portal displays?](#)
- [About monitoring remote clients from the management server](#)
- [Location awareness best practices for Endpoint Protection](#)

Finding roaming clients and critical events

To find out which clients are roaming, look for the following items:

- Whether the device is connected directly to the cloud console and not the management server.
- The location as defined in the Symantec Endpoint Protection Manager location awareness policy
- The external IP address of the client.

To find roaming clients and critical events

1. In the cloud console, go to **Incidents and Alerts**.
2. On the **Security Events** tab, under **Connection Type**, click **Cloud** to display the events that the client sends to the cloud console.

To display events that the management server sends, click **Symantec Endpoint Protection Manager**.

3. Under **Severity**, click **Critical**.

The cloud console filters and displays only the critical security events that the roaming clients detected.

4. To find the location and external IP address, select the device and look for the Device Location entry.

What are the critical events that the cloud console displays?

The roaming client uploads the following security events to the cloud console:

-
- Port scan events
 - Mac spoofing
 - Denial of service
 - Canary
 - IPS
 - Memory Exploit Mitigation
 - Host Integrity compliance

The roaming client uploads the following security events to the cloud console:

- Antivirus
- Behavioral analysis (SONAR)

Unenrolling Symantec Endpoint Protection Manager domains from the cloud server

The unenrollment process removes the client groups and clients of the unenrolled domain in the cloud. Any associated policies remain in the cloud console as well as related events.

After you unenroll a Symantec Endpoint Protection Manager domain from the Symantec Endpoint Security (SES) cloud server, you are no longer able to:

- Manage devices from the cloud console.
- See files and applications on your devices.
- Apply cloud-specific policies to devices and device groups to protect them.

During the unenrollment process, a notification appears on the cloud console and you are not able to:

- Perform any function that is associated with device management, such as creating groups, deleting groups, or moving devices between groups.
- Perform any function that is associated with policy management, such as applying policies to devices or device groups.
- Enroll a new domain until the current domain is unenrolled.

NOTE

To unenroll domains, you require the **Endpoint Console Super Administrator** role. See:

[Creating an administrator account](#)

After unenrollment, you continue to see alerts, events, and policies in the cloud console.

To unenroll a Symantec Endpoint Protection Manager domain

1. In the Symantec Endpoint Security cloud console, go to **Integration**.
2. On the **Enrollment** tab, check the **Domain Enrollment Status > Enrolled** check box and select **Unenroll**.
3. Choose an appropriate option:
 - **Unenroll** - Select this option if you only want to unenroll Symantec Endpoint Protection Manager from the cloud server.
 - **Unenroll and remove** - Select this option if you want to unenroll Symantec Endpoint Protection Manager from the cloud server and delete all discovered devices and files information.
4. Type **Unenroll** in the text box to confirm.
5. Select **Unenroll Domain**.

NOTE

Typically unenrollment takes two hours to complete.

More information

[Enrolling a Symantec Endpoint Protection Manager domain into the cloud server](#)

[Enrolling a Symantec Endpoint Protection Manager domain into the cloud server \(14.3 RU3 or later\)](#)

Licensing Symantec Endpoint Protection

Buy or renew a license and check when your license expires.

Symantec Endpoint Protection (SEP) requires a paid license to receive security content updates, product updates and versions, and access to Technical Support. After you install Symantec Endpoint Protection Manager, you have 60 days to purchase enough license seats to cover all of your deployed clients.

Table 61: How to license Symantec Endpoint Protection

Task	Description
Step 1: Purchase a license	To purchase a new license, contact your preferred reseller . For more information, go to Symantec Getting Started and scroll down to On-Premises Security Products . You must purchase a license in the following situations: • You are a new customer. • Your trial license expired. • Your paid license expired. • You deployed more clients than your license allows (over-deployed). See: What does a Symantec Endpoint Protection license cover?
Step 2: Download your license file from the Broadcom portal	Go to the Broadcom portal and download the license file (.slf) to your Symantec Endpoint Protection Manager computer. The license is no longer mailed to you.
Step 3: Activate your purchased license	You need the serial number to activate the installation. • Log on to the Symantec Endpoint Protection Manager with a system administrator account, such as the default account <code>admin</code>. • Go to the Admin > Licenses page to import and activate your Symantec Endpoint Protection product license file.

[Important Customer Information for Symantec Enterprise Division, Broadcom](#)

You can perform the following tasks to manage your licenses.

Table 62: Licensing tasks

Task	Description
Retrieve your serial number	If you have an existing license from Symantec and must retrieve your serial number, see: My Entitlements FAQ for downloading Broadcom licenses and products
Renew your license	Contact your preferred reseller . See: Purchase or renew licenses and subscriptions for Broadcom products
Find out when your license expires and if you are overdeployed	Check the status for each license that you imported into the console to see whether you must renew a license or purchase more licenses. You can apply an existing license to a product upgrade. See: When does my Symantec Endpoint Protection license expire? What happens when a license expires or is overdeployed (SEP or SES)?

Task	Description
Back up your license file	Back up your license files to preserve them in case the database or the computer hard disk becomes damaged. See: Backing up and recovering your license file (.slf)
Recover your license file	If you accidentally delete the license file, you can recover it. See: Backing up and recovering your license file (.slf)
Send notifications when licenses are expiring	By default, Symantec Endpoint Protection sends the administrator a preconfigured notification about expired licenses and other license issues. See: How do I receive a notification that my Symantec Endpoint Protection licenses are expiring?
Check the product license requirements	Learn what are the license requirements for the computers that you want to protect. A license lets you install the Symantec Endpoint Protection client on a specified number of computers. See: • What does a Symantec Endpoint Protection license cover? • Symantec Endpoint Protection product license terminology • About multi-year licenses

When does my Symantec Endpoint Protection license expire?

You can find out whether the management server uses a trial license or a paid license. You can also obtain the following license information for each paid license that you imported into the console:

- License serial number, total seat count, expiration date
- Number of valid seats
- Number of deployed seats
- Number of expired seats
- Number of over-deployed clients

The trial license status only provides limited information that is related to the expiration date.

To check when the Symantec Endpoint Protection Manager license expired

1. To check whether you have a paid license or trial license, in the console, do one of the following tasks:
 - Click **Admin > Licenses**.
 - Click **Home > Licensing Details**.
2. To check the license expiration date, in the console, click **Admin > Licenses**.

More information

- [Usage Data \(Telemetry\)](#)
- [Licensing Symantec Endpoint Protection](#)
- [Activating or importing your Symantec Endpoint Protection product license](#)

How do I receive a notification that my Symantec Endpoint Protection licenses are expiring?

If you see the message: *Symantec License Expires In 30 Days* from the Symantec Endpoint Protection Manager (SEPM), your paid licenses are about to expire and you must renew them.

By default, system administrators receive a notification when the following license events occur:

On-premises	• Paid license expiration: This notification alerts administrator and (optionally) partners. about the paid licenses expired or that are about to expire within 30 days. You cannot increase the warning time period. • Overdeployment: This notification alerts administrators and optionally partners about overdeployed paid licenses. • Trial license expiration: Trial licenses that are expired or due to expire in 60, 30, and 7 days. For other types of notifications, see: What are the types of notifications and when are they sent?
Cloud console	• Your license is about to expire or has expired. • A device reports an invalid or missing license. Using alert rules

To configure a licensing notification

1. On the **Monitors** page > **Notifications** tab, click **Notification Conditions**, and then click a notification type.
2. In the **Notification Conditions** pane, select any of the notifications and click **Edit**:
 - **Trial License Expiration**
 - **Paid License Issue**
 - **Over Deployment Issue**To add your partner's email address, add it to the **Send email to** text field.
3. Modify any of the fields as needed, and then click **OK**.

To delete a licensing notification

If you do not want the expiration notifications to appear, delete them. You can add them later if need be.

1. On the **Notifications Conditions** page, select the notification and click **Delete**.

More information

- [What happens when your SEP license expires?](#)
- [Setting up administrator notifications](#)

What happens when a license expires or is overdeployed (SEP or SES)?

This topic covers the impact for an expired or out-of-compliance Symantec Endpoint Protection (SEP) or Symantec Endpoint Security (SES) license.

You can purchase the following licenses:

- The **Symantec Endpoint Protection** license, which includes access to the on-premises Symantec Endpoint Protection only and no access to the Symantec Endpoint Security (SES) cloud console.
 - The **Symantec Endpoint Security** license, which includes access to the cloud console, and the on-premises Symantec Endpoint Protection Manager (SEPM). The SES license provides full cloud console management and hybrid management, which lets you enroll the Symantec Endpoint Protection Manager domain in the cloud. You can purchase either the Symantec Endpoint Security Enterprise (SESE) license or the Symantec Endpoint Security Complete (SESC) license, the later which provides more features.
- See: [Symantec Endpoint Security features](#)

The behavior of the license depends on whether you use the license for the on-premises SEP or the cloud console.

What does a license do?

The Symantec licenses have the following functions.

- Dictate compliance.
- Determine the product type. The product type enables certain features that you have available, such as Symantec Endpoint Security Enterprise (SESE) versus Symantec Endpoint Security Complete (SESC).
- Obtain a Client Authentication Token (CAT) from Symantec. The CAT enables the client to authenticate itself with the Symantec servers. For example, the client connects to the reputation servers for Download Insight.

How do I get a license?

Symantec Endpoint Protection

The on-premises SEP license is a software license product and uses a license file. When you first purchase a license from a partner, you receive either a product license serial number or a Symantec License file (.SLF). License files are either sent through email or downloaded from a secure web site. When you receive the license file by email, it is attached to the email as a .ZIP file; you extract the .SLF file from the .ZIP file. Save the license file to a computer that can be accessed from the Symantec Endpoint Protection Manager console. Save both:

- The license on the computer that hosts the SEPM.
- A copy of the license to a different computer or removable storage media for safekeeping.

NOTE

Sometimes you may have a license serial number only. This serial number can be used to activate your Symantec product license and to download the product software. A Symantec Endpoint Protection license applies to the Symantec Endpoint Protection clients. For instance, in a network with 50 endpoints, the license must provide for a minimum of 50 seats. Instances of the Symantec Endpoint Protection Manager do not require a license.

Symantec Endpoint Security

You must purchase a Symantec Endpoint Security Enterprise or a Symantec Endpoint Security Complete subscription to get access to the cloud. These subscriptions are hybrid, which means that once your order is provisioned, the SES Enterprise or SES Complete subscription is automatically applied to the cloud console. You do not need to activate the subscription. After you purchase SES Enterprise or SES Complete, the subscription is automatically activated in the cloud. You then sign on to <https://securitycloud.symantec.com/> to deploy the client software.

The on-premises SEP is included with a SES Enterprise or SES Complete subscription.

To get a license key, see: [Download or renew license keys for Broadcom, CA, and Symantec products](#)

To renew or purchase more seats for SES, see: [Purchasing and renewing subscriptions in Symantec Endpoint Security](#)

Consequences of an overdeployed or expired license

When the license goes out of compliance, the Symantec product goes into a *soft enforcement* mode. Soft enforcement means:

- The management console continues to download the content.
- The user interface changes and log notifications start.

In SEP, if limited administrators do not have group rights and feature rights, they cannot see reporting data and do not receive notifications. If limited administrators have both group rights and reporting rights, they receive a notification that the license is about to expire or is overdeployed.

Hard enforcement means the content updates stop.

If your paid license is overdeployed or expired, the following behaviors occur.

Management	License Type	License Status	Behavior
On-premises Symantec Endpoint Protection	Trial	Overdeployed	Allowed
		Expired	LiveUpdate content is disabled.
	Paid	Overdeployed	Allowed - The client no longer submits samples and data to Symantec Insight but clients do receive content updates. - The clients continue to submit reputation data to Insight. - The Symantec Endpoint Protection Manager generates notifications that warn the administrator of the non-compliance.
		Expired	Allowed - The client no longer submits samples and data to Symantec Insight but clients do receive content updates. - The Symantec Endpoint Protection Manager generates alerts to warn the administrator of the non-compliance. SEPM indicates when the license has expired. SEPM also displays a warning about the impending expiration about 60 days before the license expiration date. The number of days before expiration is specified in the .SLF file.
Symantec Endpoint Security cloud console	Trial	Overdeployed	Protection features are not activated on devices exceeding the trial limit of 25.
		Expired	Both LiveUpdate content* and protection features are disabled.
	Paid	Overdeployed	Allowed
		Expired	- You have 30 days to renew your license before you cannot access the cloud console, and Symantec removes the tenant and purges the data. If you renew your license within that 30 days, you get an additional 30 days after the original 30 days ends. - The cloud-managed SEP client downloads content until the tenant license expires. - Within the 30 days, you receive notifications by either email, pop-up notifications when you log on, or a persistent banner in the cloud console.

*When LiveUpdate content is disabled, antimalware real-time scans are automatically disabled on Windows 10 RS3+.

- You are still out of compliance even if the behavior is allowed.
- The cloud license that is imported into SEPM behaves the same way as the on-premises SEP license.
- SEP clients in the hybrid management mode follow the on-premises SEP license for basic features and the cloud SES license for cloud-only features. For example, a trial license in the hybrid management mode allows 25 devices only that can run Intensive Protection, App Control, and so forth. When the on-premises license expires on SEPM, SEPM discontinues content downloads. For a SEP 14.3 RU4 client, Intensive Protection and App Control continue to function on those 25 devices. However, the cloud console shows that the license has expired and is out of compliance. For a SEP 14.3 RU3 and earlier client, Intensive Protection and App Control are no longer applied.

Counting overdeployed or expired licenses

Symantec counts licenses per managed device. A *device* means a single physical or virtual desktop, laptop computer, thin client, workstation, mobile device, server, or other virtual operating system environment, on which a single instance of the software, or portion thereof, is installed, executed, or performing services.

NOTE

Servers require a SES Complete or SES Enterprise license.

In SES, the licenses are counted by policy rather than by device.

To find the number of overdeployed and expired licenses

Symantec Endpoint Protection:

1. In the console, click **Reports > Quick Reports**.
2. On the **Quick Reports** tab, select **Computer Status > Symantec Endpoint Protection Licensing Status**, and then click **Create Report**.

 Reporting - Symantec Endpoint Protection Licensing Status

 **Symantec Endpoint Protection**

Symantec Endpoint Protection Licensing Status

Report generated on: 11/18/2021 02:40:01 [Print](#) [Save](#) [Close](#)

Description: This report contains licensing status, expiration dates and deployment status.

[View License Details](#)

Deployment Summary

Total Purchased (100)	
Seats Used (2)	
Seats Available (98)	
Expired (0)	
Overdeployed (0)	

License Details

Product	Seats Used	Seats Available	Expired	Over Deployed
Symantec Endpoint Protection	2	98	0	0

Client Details

Client Type	Windows	Mac	Linux
Symantec Endpoint Protection	2	0	0

Symantec Endpoint Security:

See: [Checking the status of your Symantec product subscription](#)

How do I receive a notification that my license is overdeployed or expired?

For more information, see: [How do I receive a notification that my Symantec Endpoint Protection licenses are expiring?](#)

License behavior

The on-premises SEP and the SES cloud console use the following types of licenses for compliance.

License type	Description	On-premises	Cloud console
Trial license	- A trial license lets you evaluate the product. - Provides hard enforcement for both SEP and SES	- The SEP license is valid for 60 days. - Unlimited devices. - When you download the software, the license is included with SEPM and is activated when you configure the SEPM.	- The SES license is valid for 30 days. - A maximum of 25 devices. - Hard enforcement is temporarily suspended for 14.3 RU4 or later clients.
Paid license	You obtain and manage paid licenses from a preferred reseller on the Broadcom Licensing portal. Used to license unmanaged clients.	Imported into the SEPM console through the Admin > Licenses tab.	The Broadcom licensing team adds the license to the cloud tenant. To view the license, go to the Settings > Subscriptions tab.

Licenses do not have a grace period.

SEP and SES do not use either upgrade licenses or overdeployed licenses. If you transition from SEP to SES Enterprise or SES Complete, you purchase a new license, but you keep the same license file.

Troubleshooting

You can reclaim license seats that are not used anymore.

SEP:

You enable SEPM to remove clients that have not checked in within the past 24 hours, which makes these license seats available. If the number of installed clients is more than the license seat count, then this procedure does not resolve the issue. In that case, you must purchase more seats.

For information on how to reclaim unused licenses, see:

- [Purging obsolete clients from the database to make more licenses available](#)
- [Symantec Endpoint Protection Manager is showing over deployment of clients](#)

SES:

[Purging offline devices from Symantec Endpoint Security to make more licenses available](#)

Make more licenses available by deleting obsolete licenses

Symantec Endpoint Protection Manager can incorrectly display an over-deployed license status due to obsolete clients. These are database entries for the clients that no longer communicate with Symantec Endpoint Protection Manager in the protected environment. Clients can be rendered obsolete for many reasons, such as when you upgrade the operating system, decommission a computer, or change the hardware configuration.

If your license reports show that more seats are licensed than known to be deployed, you should remove the database of obsolete clients. Obsolete clients count against the product license, so it is important to purge obsolete clients when they are created. By default, purging occurs every 30 days. You can shorten the interval between purge cycles to more quickly purge the obsolete clients. You reset the interval to suit your long-term needs after the purge cycle completes.

In non-persistent Virtual Desktop Infrastructures (VDIs), you can set a separate time period for purging the non-persistent clients. This setting purges the offline clients that have not connected during the time period that you set. Non-persistent offline clients do not affect the license count.

NOTE

Follow this task if you installed the license on another site or location by mistake.

To delete clients from the database

1. In the console, on the **Admin** page, click **Domains**, right-click the domain, and click **Edit Domain Properties**.
2. On the **General** tab, change the **Delete clients that have not connected for specified time** setting from the default of **30** to **1**.

You do not need to set the option to purge the non-persistent clients for licensing purposes. The non-persistent clients that are offline do not count toward the license total.

3. Click **OK**.
4. Wait 24 hours and then revert the settings to 30 days or to another interval that suits your requirements.

More information

- [Purging obsolete non-persistent VDI clients to free up licenses](#)
- [Licensing Symantec Endpoint Protection](#)

What does a Symantec Endpoint Protection license cover?

The number of Symantec Endpoint Protection licenses are enforced according to the following rules:

Table 63: Licensing enforcement rules

Where applies	Rule
Term of license	The term of the license starts from the time and date of activation until midnight of the last day of the licensing term. If you have multiple sites, the license expires on the day and the time of the westernmost Symantec Endpoint Protection Manager database.
Symantec Endpoint Protection components	A Symantec Endpoint Protection license applies to the Symantec Endpoint Protection clients. For instance, in a network with 50 computers, the license must provide for a minimum of 50 seats. Instances of Symantec Endpoint Protection Manager do not require a license. Symantec Endpoint Protection Manager does not require that the client has a license to access the management server. An unlicensed client that connects to the management server is given a license. You must ensure that you have purchased enough license seats to cover each client computer.
Sites and domains	A Symantec Endpoint Protection product license is applied to an entire installation regardless of the number of replicated sites or domains that compose the installation. For instance, a license for 100 seats covers a two-site installation where each site has 50 seats. If you have not implemented replication, you may deploy the same .slf file to multiple Symantec Endpoint Protection management servers. The number of clients reporting to your management servers must not exceed the total number of licensed seats.
Platforms	License seats apply to clients running on any platform, whether the platform is Windows, Mac, or Linux.
Products and versions	License seats apply equally across product versions.

For information on licensing the clients that access the third-party server software, such as Microsoft SQL Server, contact the software vendor.

More information

-
- [Licensing Symantec Endpoint Protection](#)
 - [Purging obsolete non-persistent VDI clients to free up licenses](#)

Backing up and recovering your license file (.slf)

You should back up your license file in case the database or the console computer's hard disk becomes damaged.

After you receive the license file, save it to a computer that can be accessed from the Symantec Endpoint Protection Manager console. Many users save the license on the computer that hosts Symantec Endpoint Protection Manager. Many users also save a copy of the license to a different computer or removable storage media for safekeeping.

To back up your license file

1. Copy the **.slf** license files from the directory where you saved the files to another computer of your choice.

To recover your license file

- Do one of the following tasks:
 - a. On the Symantec Endpoint Protection Manager console **Admin** page, click **Licenses** and then under **Tasks**, click **Recover a deleted license**. On the **License recovery** panel, check the box next to the deleted license you want to recover, and then click **Submit**.
 - b. Retrieve the license file from the following default location: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\inetpub\license. When you import the license file using the Licensing Activation Wizard, Symantec Endpoint Protection Manager places a copy of the file in this folder.
 - c. Go to the [Symantec Endpoint Security](#) website, and click **My Entitlements**. For more information, see: [Symantec to Broadcom Transition Guide - My Entitlements](#)

More information

[Licensing Symantec Endpoint Protection](#)

About multi-year licenses

When you purchase a multi-year license, you receive a set of license files equal to the number of years your license is valid. For instance, a three-year license consists of three separate license files. When you activate a multi-year license, you import all of the license files during the same activation session. Symantec Endpoint Protection Manager merges the separate license files into a single activated license that is valid for the purchased duration.

While not recommended, it is possible for you to activate fewer than the full complement of license files. In this case, Symantec Endpoint Protection Manager merges the files and applies the duration of the license file that expires last. For instance, a three-year license that is activated with only the first two files indicates a duration of only two years. When you activate the third file at a later date, Symantec Endpoint Protection Manager accurately reports the full duration of the license as three years. In all cases, the number of seats remains consistent with the number of seats that you purchased.

When Symantec Endpoint Protection Manager merges files, it deletes the shortest duration files and keeps the longest duration file for internal license-keeping functions. If you think that Symantec Endpoint Protection Manager inappropriately deleted a license, recover and reactivate the deleted license.

You can see the license serial numbers of shorter duration that are associated with the active license. On the **Admin** page, click **Licenses** and then click the activated license. The associated licenses appear in the **Associated Licenses** column.

More information

[Licensing Symantec Endpoint Protection](#)

Symantec Endpoint Protection product license terminology

You must purchase a license that covers each deployed client. One license covers all clients regardless of platform and version.

The following terminology applies to Symantec product licenses:

Table 64: Product license terminology

Term	Description
Serial number	A license contains a serial number that uniquely identifies your license and associates the license with your company. The serial number can be used to activate your Symantec Endpoint Protection license.
Deployed	Deployed refers to the endpoint computers that are under the protection of the Symantec Endpoint Protection client software. For example, "We have 50 deployed seats" means that 50 endpoints have client software installed on them.
Activate	You activate your Symantec Endpoint Protection product license to enable unrestricted access to all program functionality. You use the License Activation wizard to complete the activation process. See: Activating or importing your Symantec Endpoint Protection product license
Seat	A seat is a single endpoint computer that the Symantec Endpoint Protection client software protects. A license is purchased and is valid for a specific number of seats. "Valid seats" refers to the total number of seats that are specified in all of your active licenses.
Trial license	A trial license refers to a fully functioning installation of Symantec Endpoint Protection operating within the free evaluation period. If you want to continue using Symantec Endpoint Protection beyond the evaluation period, you must purchase and activate a license for your installation. You do not need to uninstall the software to convert from trialware to a licensed installation. You must get trial license from your sales account representative. The evaluation period is 60 days from the initial installation of Symantec Endpoint Protection Manager.
Over-deployed	A license is over-deployed when the number of deployed clients exceeds the number of licensed seats.

Understanding license requirements is part of planning your Symantec Endpoint Protection installation and managing your product licenses after installation.

More information

[Licensing Symantec Endpoint Protection](#)

Licensing an unmanaged Windows client

Unmanaged clients do not require the manual installation of a license file, and they do not count towards the total seat count for a paid license. However, to enable the submission of reputation data from an unmanaged Windows client, you must install a paid license on the unmanaged client. Unmanaged Mac clients and Linux clients do not submit reputation data.

To license an unmanaged Windows client

1. Locate and create a copy of your current Symantec Licensing File (.slf).
Use the same file that you used to activate your license on Symantec Endpoint Protection Manager.
2. In the client computer, place the copied license file into the Symantec Endpoint Protection client inbox (default location):

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\

By default, the folder in which the inbox appears is hidden, so use Folder Options to enable the showing of hidden files and folders.

If the license file is invalid or the license installation failed, the license appears in a new folder called `Invalid`. If the file is valid, it is automatically removed from the inbox after it is processed.

3. To verify that you applied the license correctly, check that no files appear in the inbox folder.
4. Check that the `.slf` file is in the following folder (default location):

`C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config`

You can also include the `.slf` file as part of a third-party deployment package.

Using Policies to Manage Security

Use policies to manage the security on your client computers.

You use different types of security policies to manage your network security. Default policies are automatically created during the installation. You can use the default policies or you can customize policies to suit your specific environment.

Best practices for stopping malware and other threats

The threat landscape has changed and cybercrime is rampant. Companies cannot depend solely on desktop antivirus technology to protect themselves.

Must do

Follow these steps to improve the protection of desktops and to stop malware using Symantec Endpoint Protection (SEP).

- **Use IPS (Intrusion Prevention System):** Threats today are web-based. The IPS in Symantec Endpoint Protection stops threats before they can infiltrate a machine. IPS stops vulnerability exploits, drive-by-downloads, and fake antivirus installation.
- **Improve the default Symantec Endpoint Protection settings:** Get the most out of your Symantec Endpoint Protection product by improving its default settings. Only a few setting changes can make a big improvement to your security.
- **Keep browser plugins patched:** Attacks have moved to the browser. It is critical that attackers do not use Microsoft Internet Explorer, or Adobe Reader/Acrobat/Flash vulnerabilities to get on a system. Use each vendor's auto update or software distribution tools to install patches when they become available.
- **Block P2P usage:** The simplest method for distributing malware is hidden inside files be shared on peer-to-peer (P2P) networks. Create and enforce a no-P2P policy, including home usage of a company machine. Enforce the policy at the gateway and/or desktop. [Learn more about using Symantec Endpoint Protection to block P2P at the desktop](#)
- **Turn off AutoRun:** Stop Conficker/Downadup and other network-based worms from jumping from USB keys and network drives without changing company policies on Open Shares.

Should do

- **Turn on enhanced security in Adobe Reader:** Protect your machines from attacks hidden in PDF files by hardening Adobe Reader. [Learn more about using the enhanced security settings available in Reader.](#)
- **Limit the use of network shares (mapped drives):** Worms love to spread through networked drives. Unless there is a strong business requirement, close mapped drives. If possible limit permissions to read-only rather than read-write.
- **Review mail security and gateway blocking effectiveness:** Catch threats before they get to the desktop by using effective mail and web security scanning. Check that you have a mail security solution which updates frequently to detect the latest bad sender IPs, spam, and malware threats at the mail gateway. Consider implementing a web security solution that protects your organization against Web 2.0 threats, including malicious URLs and malware.
- **Review your security content distribution schedule:** Antivirus signatures are released multiple times a day and IPS content roughly on a weekly basis or as needed. If possible, take advantage of these updates or at least update machines that are frequently infected.
- **Review your security content distribution schedule:** Administrators sometimes deploy SEP with only the traditional signature-based virus and spyware component. The additional optional components (Network Threat Protection, Intrusion Prevention System, Application and Device Control, Proactive Threat Protection) greatly enhance SEP's ability to defend against today's sophisticated threats. The Insight technology is particularly effective against the very latest threats for which no virus signatures yet exist. Unless there is a compelling reason to, each of these additional components should be deployed throughout the organization. See: [Add or remove features to existing Endpoint Protection clients](#)

Can do

- **Implement application control rules to block specific threats:** Application and Device Control is a power tool that can be used to stop a specific file, block peer-to-peer (P2P) network use or protect critical files and registry entries.
- **Educate users:** Most malware attacks use social engineering. Education can be highly effective in stopping them. Your users do not need to be security experts. Today, just remembering four things can keep them protected.
 - Only click through to trusted sources when conducting searches, especially on topics with high attention.
 - Never update the media player, codec, or Flash software from a site that hosts videos or that is not affiliated with that application.
 - Do not use P2P applications on business machines and be cautious on home machines.
 - Do not click links or attachments in spam email.
- **Educate yourself:** Symantec provides [multiple resources](#) to keep you up to date on the latest security threats.
 - [P2P Blocking](#)
 - [SEO Poisoning](#)

Ransomware mitigation and protection with Symantec Endpoint Protection

What is ransomware?

Ransomware is a category of malware that encrypts documents, which makes them unusable, and leaves the rest of the computer accessible. Ransomware attackers try to force their victims to pay a ransom through specifically noted payment methods after which they may or may not grant the victims access to their data.

Targeted ransomware is more complex than the original ransomware attacks and involves more than just the initial infection. Attackers have found more ways of extorting victim organizations using the following range of distribution methods:

- **Phishing:** Emails sent to employees disguised as work-related correspondence.
- **Malvertising:** Compromising media websites in order to serve malicious ads containing a JavaScript-based framework known as SocGhosh which masquerades as a software update.
- **Vulnerability exploitation:** Exploiting vulnerable software running on public-facing servers.
- **Secondary infections:** Leveraging pre-existing botnets in order to gain a foothold on the victim's network.
- **Poorly secured services:** Attacking organizations through poorly secured RDP services, taking advantage of leaked or weak credentials.

Protecting against ransomware with Symantec Endpoint Protection

Most of the features to protect against ransomware in Symantec Endpoint Protection, are enabled by default. For more information on which features protect your environment, see:

[Ransomware protection using Symantec Endpoint Protection](#)

[Protecting against ransomware with Symantec Endpoint Security](#)

[Ukraine: Disk-wiping Attacks Precede Russian Invasion](#)

Best practices to mitigate ransomware

[Hardening Your Environment Against Ransomware](#)

In addition to enabling SEP protection, follow additional steps to avoid ransomware infection.

Table 65: Steps to avoiding ransomware

Step	Action
1. Protect your local environment	Ensure you have the latest version of PowerShell and that you have logging enabled. Restrict access to RDP services. Only allow RDP from specific known IP addresses, and ensure you are using multi-factor authentication. Use File Server Resource Manager (FSRM) to lock out the ability to write known ransomware extensions on file shares where user write access is required. Create a plan to consider notification of outside parties. In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place to verify. Create a “jump bag” with hard copies and archived soft copies of all critical administrative information. In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted. Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and usage of admin credentials. Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network. A user account that has a history of running as admin using PsInfo/PsExec on a small number of systems is probably fine, but a service account running PsInfo/PsExec on all systems is suspicious.
2. Protect your email system	- Enable two-factor authentication (2FA) to prevent compromise of credentials during phishing attacks. Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.
3. Make backups	Regularly back up the files on both the clients and servers. Either back up the files when the computers are offline or use a system that networked computers and servers cannot write to. If you do not have dedicated backup software, you can also copy the important files to removable media. Then eject and unplug the removable media; do not leave the removable media plugged in. Implement offsite storage of backup copies. Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups. Implement offline backups that are onsite. Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware. Removal is best done with the system off the networks to prevent any potential spread of the threat. Verify and test your server-level backup solution. This should already be part of your disaster recovery process. Secure the file-level permissions for backups and backup databases. Don't let your backups get encrypted. Test restore capability. Ensure restore capabilities support the needs of the business. Lock down mapped network drives by securing them with a password and access control restrictions. Use read-only access for files on network drives, unless it is absolutely necessary to have write access for these files. Restricting user permissions limits which files the threats can encrypt.

What should you do if you get ransomware?

There is no ransomware removal tool. No security product can decrypt files that ransomware encrypts. Instead, if your client computers do get infected with ransomware and your data is encrypted, follow these steps:

1. Do not pay the ransom.

If you pay the ransom:

- There is no guarantee that the attacker will supply a method to unlock your computer or decrypt your files.
 - The attacker uses the ransom money to fund additional attacks against other users.
2. **Isolate the infected computer before the ransomware can attack network drives to which it has access.**
 3. **Use Symantec Endpoint Protection Manager or SES to update the virus definitions and scan the client computers.**
 New definitions are likely to detect and remediate the ransomware. Symantec Endpoint Protection Manager automatically downloads virus definitions to the client, as long as the client is managed and connected to the management server or cloud console.
 - In Symantec Endpoint Protection Manager, click **Clients**, right-click the group, and click **Run a command on the group > Update Content and Scan**.
 - In Symantec Endpoint Security, run the **Scan Now** command. See: [Running commands on client devices](#)
 4. **Reinstall using a clean installation.**
 If you restore encrypted files from a backup, you can get your restored data but it's possible that other malware was installed during the course of the attack.
 5. **Submit the malware to Symantec Security Response.**
 If you can identify the malicious email or executable, submit it to Symantec Security Response. These samples enable Symantec to create new signatures and improve defenses against ransomware. See: [Symantec Insider Tip: Successful Submissions!](#)

Ransomware protection using Symantec Endpoint Protection

Targeted ransomware attacks can be broken down into the following broad phases:

- Initial compromise
- Privilege escalation and credential theft
- Lateral movement
- Encryption and deletion of backups

The best defense is to block the many types of attacks and know the attack chain that most cyber crime groups use to identify security priorities. Unfortunately, ransomware decryption is not possible using removal tools.

On Symantec Endpoint Protection Manager, deploy and enable the following features. Some features are enabled by default.

Table 66: Symantec Endpoint Protection Manager features

Step	Action
Step 1: Enable file-based protection Symantec quarantines the following types of files: Ransom.Maze, Ransom.Sodinokibi, and Backdoor.Cobalt	Enable the Virus and Spyware Protection policy, which is enabled by default. See: Preventing and handling virus and spyware attacks on client computers
Step 2: Enable Behavioral Analysis (SONAR) Symantec Endpoint Protection's behavioral-based protection is another crucial defense against malware. SONAR prevents the double executable file names of ransomware variants like CryptoLocker from running.	In a Virus and Spyware Protection policy, click SONAR > Enable SONAR . This option is enabled by default. See: Managing Behavioral Analysis (SONAR)

Step	Action
Step 3: Modify Download Insight Symantec Insight prevents ransomware variants by quarantining the files that the Symantec customer base knows are malicious or that haven't yet been proven to be either safe or malicious.	Download Insight is part of the default Virus and Spyware - High Security policy. 1. In the console, open the target Virus and Spyware Protection policy and click Download Protection. If adding a new policy, select the Virus and Spyware Protection policy - High Security policy. 2. On the Download Insight tab, make sure that Enable Download Insight to detect potential risks in downloaded files based on file reputation is checked. 3. Check the following default options: — Files with 5 or fewer users — Files known by users for 2 or fewer days The low default values force the client to treat any file that has not been reported to Symantec by more than five users or for less than 2 days to be treated as unproven files. When unproven files meet these criteria, Download Insight detects the files as malicious. 4. Make sure that Automatically trust any file downloaded from a trusted Internet or intranet site is checked. 5. On the Actions tab, under Malicious Files, keep the first action as Quarantine risk and the second action as Leave alone. 6. Under Unproven Files, click Quarantine risk. 7. Click OK.
Step 4: Enable the Intrusion Prevention System (IPS) • IPS blocks some threats that traditional virus definitions alone cannot stop. IPS is the best defense against drive-by downloads, which occurs when software is unintentionally downloaded from the Internet. Attackers often use exploit kits to deliver a web-based attack like CryptoLocker through a drive-by download. • In some cases, IPS can block file encryption by interrupting command-and-control (C&C) communication. A C&C server is a computer controlled by an attacker or cybercriminal and that is used to send commands to systems compromised by malware and receive stolen data from a target network. • URL reputation prevents web threats based on the reputation score of a web page. The Enable URL Reputation option blocks web pages with reputation scores below a specific threshold. (14.3 RU1 and later).	For more information, see: Enabling network intrusion prevention or browser intrusion prevention URL reputation is enabled by default.
Step 5: Block PDF files and scripts	In the Exceptions policy, click Windows Exceptions > File Access.

Step	Action
Step 6: Download patches Download the latest patches for web application frameworks, web browsers, and web browser plug-ins.	Do the following: 1. Use the Application and Device Control to prevent applications from running in the User Profile directories, such as Local and LocalLow. Ransomware applications install themselves into many directories apart from Local\Temp\Low. See: Strengthening anti-virus security to prevent Ransomware derivative (Trojan.Cryptolocker family, etc.) infections 2. Use Endpoint Detection Response (EDR) to identify files with ransomware behavior: a. Disable macro scripts from MS Office files that are transmitted through email. b. Right-click the detected endpoints and select Isolate. To isolate and rejoin endpoints from the console, you must have a Quarantine Firewall policy in Symantec Endpoint Protection Manager that is assigned to a Host Integrity policy. See: About Host Integrity and Quarantine Firewall Policies
Step 7: Enable Web and Cloud Access Protection and Symantec Cloud Secure Web Gateway (Cloud SWG) Use Web and Cloud Access Protection and secure connection settings so that whether on a corporate network, at home or out of office, endpoints have the ability to integrate with the Cloud SWG. Web and Cloud Access Protection redirects Internet traffic on the client to the Cloud SWG, where the traffic is allowed or blocked based on the Cloud SWG policies.	For more information, see: Controlling Internet access with Web and Cloud Access Protection
Step 8: Enable Memory Exploit Mitigation Protects against known vulnerabilities in unpatched software, such as JBoss or Apache web server, which attackers exploit.	For more information, see: Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy
Step 9: Enable AMSI and file-less scanning Third-party application developers can protect their customers from dynamic script-based malware and from non-traditional avenues of cyberattack. The third-party application calls the Windows AMSI interface to request a scan of user-provided script, which is routed to the Symantec Endpoint Protection client. The client responds with a verdict to indicate on whether or not the script behavior is malicious. If the behavior is not malicious, then the script execution proceeds. If the script's behavior is malicious, the application does not run it. On the client, the Detection Results dialog box displays a status of "Access Denied." Examples of third-party scripts include Windows PowerShell, JavaScript, and VBScript. Auto-Protect must be enabled. This functionality works for Windows 10 and later computers. 14.3 and later.	Enabled by default. See: • How the Antimalware Scan Interface (AMSI) helps you defend against malware • Antimalware Scan Interface (AMSI)

Step	Action
Step 10: Enable Endpoint Detection and Response (EDR) EDR focuses on behaviors rather than files and can strengthen defenses against spear phishing and use of living-off-the-land tools. For example, if Word doesn't normally launch PowerShell in the customer environment, then this should be placed in Block mode. EDR's UI allows customers to easily understand which behaviors are common and should be allowed, which are seen but should still be alerted on, and which are uncommon and should be blocked. You can also address gaps reactively as part of investigating and responding to incident alerts. The incident alert will show all behaviors that were observed as part of the breach and provides the capability to put this in block mode right from the incident details page.	For more information, see: Configuring client groups to use private servers for reputation queries and submissions
Step 11: Enable auditing Use auditing tools to help you gain insight into your endpoints both on a corporate network and outside of your corporate network before ransomware has a chance to spread.	Use Memory Exploit Mitigation to test for false positives. See: Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy
Step 12: Set up unmanaged detectors Unmanaged detectors need to be present to account for endpoints where protection may not be present.	For more information, see: Configuring a client to detect unmanaged devices

More information

[Ransomware removal and protection with Symantec Endpoint Protection](#)

What's new in ransomware protection against living-off-the-land techniques (SEP and SES)

Symantec Endpoint Protection (SEP) and Symantec Endpoint Security (SES) include enhancements that protect your client computers against living-off-the-land (LotL) tools as well as files, network tools, and other general attack tools available in the malware market.

Living-off-the-land tactics—where attackers take advantage of native tools and services already present on targeted systems—have been used by both targeted attack groups and common cyber criminal gangs.

The following technologies protect against targeted ransomware threats.

14.3 RU9

- Updated protection for following ransomware threats:
Akira, Alabat, Babuk, BiBi wiper, Black Basta, Blackcat, BlackHunt, BlackSuit, DoNex, Freeworld, Hunter International, Inc, Knight, Kuiper, Lockbit, Medusa, Mimic, Qilin, Phobos, Phoenix, Stop, Trigona, the Tuga ransomware families, and various tools used in ransomware attacks.
- Endpoint network protection was improved for various pre-ransomware and exfiltration tools including impacket, MegaSync, FileZilla, and WinSCP.

14.3 RU8

- Updated protection against the following ransomware threats:
Akira, Bianlin, Blackbyte, Blackcat, BlackBasta, Crosslock, Hardbit, Hsharada, IceFire, Lockbit, Magniber, Moneybird, Moneymessage, Noberus, Nokoyawa, Rancoz, Royal, and various tools used in ransomware attacks.
- Updated protection against the following malware:

Qakbot, AgentTesla, Gopuram, Icedid, Malicious Chrome WebExtensions, VipersoftX, Xworm.

- Improved the Attack Group Remediation (AGR) feature to support termination of more processes. AGR identifies all the components in a detected attack and ensures that each process and thread that is part of the attack is removed.
- Enhanced scanning flow for MSI malwares.
- Enhanced emulation support for VBA downloaders used by IcedID.
- Released a new detection framework for PDF malware.
- Improved OneNote parser to extract additional file types.

14.3 RU7

- Hardbit, IceFire, Lockbit, Magniber, Moneymessage, Noberus, Nokoyawa, Royal, and various pre-ransomware tools.

14.3 RU6

Network protection technologies

- Improved network protection for ransomware families such as Conti, Avoslocker, and Hive.
- Improved network detection and protection against pre-ransomware tools that are used in ransomware attacks.
- Improved network detection and protection against initial access and lateral movement techniques that are used in ransomware attacks.

File inspection technologies

- Improved emulation and heuristics for LNK threats.
- Improved emulation and heuristics for HTML threats such as Qakbot and Gamaredon.
- Improved emulation and heuristics for BAT scripts that are used in pre-ransomware activities.
- Improved PowerShell emulation for pre-ransomware activities.
- Improved engine capability for VBA extraction and VBE/JSE decoding.
- Enabled non-PE cloud lookup to boost the efficacy for non-PE threats.

Behavioral protection

- Improved heuristic detection for renamed LotLBins.
- Improved BASH memory scan performance and efficacy (ransomware, Cobalt Strike).
- Improved thread injection protection for threats such as Bumblebee.
- Improved BPE coverage for threats with a large file size.
- AEP and JESE scan flow enhancement to deal with Qakbot, which leverages the svg attribute to drop the payload.
- Improved generic ransomware BPE detections to mitigate the big loop, multi-threading, and exoneration issues.

14.3 RU5

Network protection technologies

- Improved network protection for ransomware families like Conti, Avoslocker, and Hive.
- Improved network detection and protection against preransomware tools that are used in ransomware attacks.
- Improved network detection and protection against initial access and lateral movement techniques that are used in ransomware attacks.

Behavioral protection

- Improved generic ransomware BPE detections to mitigate the big loop, multi-threading, and exoneration issues.

14.3 RU4

Network protection technologies

-
- Improved network protection for ransomware families like Conti, AvosLocker, and Hive.
 - Improved network detection and protection against preransomware tools that are used in ransomware attacks.
 - Improved network detection and protection against initial access and lateral movement techniques that are used in ransomware attacks.

File inspection technologies

- Robust protections using analytics to curtail abuse of Red Team tools by malware actors.
- Created two more command-line subscanners (wbadmin.exe and wevtutil.exe) to improve the preransomware activity detection.
- Improved repair capability for Macro file infectors.
- Improved Macro extraction support for PowerPoint threats.

Behavioral protection

- Improved static and behavioral detection for Python-based ransomware.
- Enabled a BASH memory scan in the DLL format for ransomware families such as Conti. Conti ransomware loads an encrypted DLL into memory and then executes it.
- Improved preransomware activity detection for hack tools and LOLBins by creating four new command-line subscanners and multiple new detections. LOLBins are a sophisticated threat and detecting them requires advanced tools.
- Improved scoring heuristic and AMSI detection for Emotet spam campaigns.
- Enhanced memory scans with SONAR Behavioral Policy Enforcement (BPE) to handle process injection techniques that Cobalt Strike uses.

14.3 RU3

Network protection technologies

- Detection of suspicious process chains that are used in targeted ransomware attacks.
- Telemetry enhancement that sends alerts when ransomware or pre-ransomware tools impacts a new client computer.
- Protection against Cobalt Strike post-exploitation actions and lateral movements.
- Protection against high-prevalence malware such as IcedID.

File inspection technologies

- Protection that encrypts Office Open XML (OOXML), Windows Management Instrumentation (WMI), dotnet, and XLM with Antimalware Scan Interface (AMSI).
- Microsoft PowerShell emulation heuristic improvements that use AMSI disable techniques to detect malware.
- Enhanced command-line heuristics to protect against ransomware and Cobalt Strike hacking tools.
- Added PE Emulator post scan support to improve detections of malware with junk loop and anti-emulation tricks.
- Visual Basic (VB) and dotnet emulator enhancements to protect against malware like Mass Logger, FormBook, and Agent Tesla.
- Implemented the Microsoft Office Scanner to detect VBA stomping and the non-PE dropper like Hancitor.
- Includes a common parser to support VBA extraction and emulation from the Microsoft Publisher and Microsoft Access files.
- Enhanced the AMSI and Script Emulation string scan to identify and remediate LotL malware like IsErlk.

Behavioral protection

-
- Enhanced credential theft protection by stripping the read access on lsass.exe.
 - Enhanced ransomware protection by locking down file write access when ransomware detections are triggered on trusted processes.
 - Enhanced process tracking for the parent process spoofing technique.
 - Detection on process hollowing techniques by comparing the entry point address of the main thread with the entry point address that is parsed from the on-disk file.
 - Detection of suspended process creation.
 - Behavior detection for high-profile ransomware such as Ryuk, REvil/Sodinokibi, Conti, Darkside, Burglar, and Lorenz.
 - Generic ransomware pre-encryption behavior detection and post-encryption detection that leverages the new attributes for the file rename event.
 - Behavior detection of the Cobalt Strike post-exploitation actions and lateral movements, and memory detection for the Cobalt Strike beacon.
 - Behavior detection of the DLL refreshing and the process injection techniques by using the SetThreadContext function and permission flags at process handle opening.
 - Behavior detection of Microsoft Office Excel and Microsoft Office PowerPoint threats.
 - Symantec Endpoint Detection and Response (SEDR) visibilities that convert a few of the BPE detections to Advanced Attack Techniques (AAT).
 - New ACM events on LoLBins.

How do I block websites with Symantec Endpoint Protection?

SEP provides multiple features to block websites that are malicious, contain too many ads, or that are inappropriate for the workplace.

Most of the following features block the entire website, rather than a specific URL. The URL is the address that is used to access a specific resource on the Internet.

- **Web and Cloud Access Protection**

Web and Cloud Access Protection is a redirection component that gets Internet traffic, including websites, to the Symantec Cloud SWG. On Cloud SWG, you set up policies that manage and control traffic. These traffic policies block categories of websites that are deemed inappropriate in the work environment or are known sources of malicious content. You can also add unique URLs to the Cloud SWG allow list and block list, which overrides the categories that Symantec assigns.

You must configure the Web and Cloud Access Protection policy and the Cloud SWG policy.

More information

For information about defining policies, see: [Cloud SWG Policies](#)

For information about updating Cloud SWG allow and block lists, see: [Define Object Lists to Use in Custom Cloud SWG Policy](#)

[Create Custom Cloud SWG Content Filtering Rules](#)

For information about the Web and Cloud Access Protection policy, see:

SEP: [Controlling Internet access with Web and Cloud Access Protection](#)

SES: [Getting started with Web and Cloud Access Protection](#) and [Web and Cloud Access Protection FAQs](#)

- **Browser Intrusion Prevention**

The IPS browser extensions for Google Chrome and Microsoft Edge intercept VBScript, JavaScript, and ActiveX calls running in the browser as they are executed, inspecting the parameters of these calls for exploits of vulnerabilities. The Browser IPS engine then detects exploit code which would otherwise have been hidden or obfuscated from other detection methods, including the CIDS engine. The client then redirects users to a default landing page that blocks access to the URL.

Browser Intrusion Prevention is enabled by default.

[Integrating browser extensions with Symantec Endpoint Protection \(SEP\) to protect against malicious websites](#)

- **URL reputation**

URL reputation identifies threats from domains and URLs, which can host malicious content like malware, fraud, phishing, and spam. URL reputation blocks access to the web addresses that are identified as known sources of the malicious content.

URL reputation is enabled by default.

SEP: [Managing intrusion prevention](#)

SES: [Managing intrusion prevention in Symantec Endpoint Security](#)

- **IPS signatures**

IPS signatures look at the traffic to/from a website instead of looking at the website itself.

IPS signatures are installed by default.

SEP: [About Symantec IPS signatures](#)

- **Firewall rules**

You can add a firewall rule to block traffic to and from specific DNS names, such as `https://www.maliciouscompany.com`, rather than specific URLs. This method does not block websites that are accessed through an HTTP/HTTPS proxy.

For information about blocking websites with the firewall, see: [How to block specific Web sites using the Symantec Endpoint Protection \(SEP\) client Network Threat Protection \(NTP\) component](#)

Performing the tasks that are common to all policies

Your security policies define how the protection technologies protect your computers from known and unknown threats.

You can manage your Symantec Endpoint Protection security policies in many ways. For example, you can create copies of the security policies and then customize the copies for your specific needs. You can lock and unlock certain settings so that users cannot change them on the client computer.

Table 67: Tasks common to all policies

Task	Description
Add a policy	If you do not want to use one of the default policies, you can add a new policy. You can add shared policies or non-shared policies. Note: If you add or edit shared policies in the Policies page, you must also assign the policies to a group or location. Otherwise those policies are not effective. For more information, see: • The types of security policies • About shared and non-shared policies • Adding a policy
Lock and unlock policy settings	You can allow or prevent client users from configuring some policy settings and client user interface settings. See: Preventing users from disabling protection on client computers
Edit a policy	If you want to change the settings in an existing policy, you can edit it. You can increase or decrease the protection on your computers by modifying its security policies. You do not have to reassign a modified policy unless you change the group assignment. See: Editing a policy
Assign a policy	To put a policy into use, you must assign it to one or more groups or locations. See: Assigning a policy to a group or location
Test a policy	Symantec recommends that you always test a new policy before you use it in a production environment.
Update the policies on clients	Based on the available bandwidth, you can configure a client to use push mode or pull mode as its policy update method. See: Updating policies and content on the client using push mode or pull mode

Task	Description
Replace a policy	You can replace a shared policy with another shared policy. You can replace the shared policy in either all locations or for one location. See: Replacing a policy
Copy and paste a policy	Instead of adding a new policy, you may want to copy an existing policy to use as the basis for the new policy. You can copy and paste policies on either the Policies page or the Policies tab on the Clients page. Note: You can also copy all the policies in a group and paste them into another group, from the Policies tab on the Clients page. For more information, see: • Copying and pasting a policy on the Clients page • Copying and pasting a policy on the Policies page
Convert a shared policy to a non-shared policy	You can copy the content of a shared policy and create a non-shared policy from that content. See: About shared and non-shared policies A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing non-shared policy. You can convert a shared policy to a non-shared policy if the policy no longer applies to all the groups or all the locations. When you finish the conversion, the converted policy with its new name appears under Location-specific Policies and Settings. See: Converting a shared policy to a non-shared policy
Export and import a policy	You can export an existing policy if you want to use it at a different site or management server. You can then import the policy and apply it to a group or to a specific location. See: Exporting and importing individual Endpoint Protection policies
Withdraw a policy	If you delete a policy, Symantec Endpoint Protection Manager removes the policy from the database. If you do not want to delete a policy, but you no longer want to use it, you can withdraw the policy instead. You can withdraw any type of policy except a Virus and Spyware Protection policy and a LiveUpdate Settings policy . See: Unassigning a policy from a group or location
Delete a policy	If a policy is assigned to one or more groups and locations, you cannot delete it until you have unassigned it from all the groups and locations. You can also replace the policy with another policy
Check that the client has the latest policy	You can check whether the client has the latest policy. If not, you can manually update the policy on the client. See: • Using the policy serial number to check client-server communication • Updating client policies

The types of security policies

You use several different types of security policies to manage your network security. Most types of policies are automatically created during the installation. You can use the default policies or you can customize policies to suit your specific environment.

Table 68: Security policy types

Policy type	Description
Virus and Spyware Protection policy	The Virus and Spyware Protection policy provides the following protection: • Detects, removes, and repairs the side effects of virus and security risks by using signatures. • Detects the threats in the files that users try to download by using reputation data from Download Insight. • Detect the applications that exhibit suspicious behavior by using behavioral analysis (SONAR) heuristics and reputation data. The Virus and Spyware Protection policy finds behavior anomalies through its behavioral analysis technology. Note: Download Insight and behavioral analysis are available only on Windows clients. For more information, see: Managing scans on client computers
Firewall policy	The Firewall policy provides the following protection: • Blocks the unauthorized users from accessing the computers and networks that connect to the Internet. • Detects the attacks by hackers. • Eliminates the unwanted sources of network traffic. Note: Firewall policies can be applied only to Windows clients. For more information, see: Managing firewall protection
Intrusion Prevention policy	The Intrusion Prevention policy automatically detects and blocks network attacks and attacks on browsers as well as protects applications from vulnerabilities. See: Managing intrusion prevention
Application and Device Control	The Application and Device Control policy protects a system's resources from applications and manages the peripheral devices that can attach to computers. See: Setting up application control Application Control policy can be applied only to Windows clients. The Device Control policy applies to Windows and Mac computers.
Host Integrity	The Host Integrity policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. You use this policy to verify that the clients that access your network run the antivirus software, patches, and other application criteria that you define. See: Setting up Host Integrity
LiveUpdate policy	The LiveUpdate Content policy and the LiveUpdate Settings policy contain the settings that determine how and when client computers download content updates from LiveUpdate. You can define the computers that clients contact to check for updates and schedule when and how often client computers check for updates. See: How to update content and definitions on the clients
Memory Exploit Mitigation	The Memory Exploit Mitigation policy stops exploit attempts against both known and unknown vulnerabilities on software using mitigation techniques such as DLL hijacking, heap spray mitigation, and Java exploit prevention. See: Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy

Policy type	Description
Web and Cloud Access Protection	Web and Cloud Access Protection sends network traffic to a Symantec Cloud Secure Web Gateway (Cloud SWG). The Cloud SWG solution protects users and organizations by categorizing applications and web sites, and then allowing or denying access to them based on policy. Symantec Cloud Secure Web Gateway was renamed from Symantec Web Security Service in 2022. See: Controlling Internet access with Web and Cloud Access Protection
Exceptions	The Exceptions policy provides the ability to exclude applications and processes from detection by the virus and spyware scans and by behavioral analysis. You can also exclude applications from application control. See: Managing exceptions in Symantec Endpoint Protection

More information

[Performing the tasks that are common to all policies](#)

Updating security policies on the Windows client

If you do not think you have the latest policy, you can manually update the policy on the Symantec Endpoint Protection client computer.

- If policy settings prevent you from opening the user interface or the notification area icon, you may not be able to manually update the policy. No command exists in Symantec Endpoint Protection Manager to manually prompt the client to update policies.
- The client checks for policy updates that are based on its update method of pull mode or push mode.
- If the client does not receive the update, there might be a communication problem. Check the policy serial number to check whether your managed client computers can communicate with the management server.

To update the client policy

1. In the Windows taskbar, in the notification area, right-click the Symantec Endpoint Protection icon, and click **Update Policy**.
2. In the client, click **Help > Troubleshooting > Management**, and then click **Update**.

To export and import the client policy from a different client

If the client is not connected to the Symantec Endpoint Protection Manager, you should export the policy.xml file from a different client that is connected, and then import the policy.

1. In the client that connects to the management server, click **Help > Troubleshooting > Management**.
2. In the **Management** panel, under **Policy Profile**, click **Export**, and save the policy.xml to a location that you can access from the second client.
3. On the second client, click **Help > Troubleshooting > Management**, and then click **Import**. Locate the policy from the first client and follow the prompts.

Creating a custom Symantec Endpoint Protection Manager policy

Create your own custom Symantec Endpoint Protection Manager policies.

Symantec Endpoint Protection Manager comes with a default policy for each type of protection. But you can create your own custom policies. And you can create multiple versions of each type of policy.

Symantec recommends that you test all new policies before you use them in a production environment.

To create a custom policy

-
1. In the console, click **Policies**.
 2. On the **Policies** page, select a policy type, and then click the link to add a new policy.
 3. Modify the policy settings to increase or decrease protection.
 4. Click **OK** to save the policy.
 5. Optionally assign the new policy to a group.

You can assign a new policy to a group during or after the policy creation. The new policy replaces the currently assigned policy of the same protection type. See:

[Assigning a policy to a group or location](#)

More information

[Performing the tasks that are common to all policies](#)

Editing a policy

You can edit shared and non-shared policies on the **Policies** tab on the **Clients** page as well as on the **Policies** page. Locations as well as groups can share the same policy. You must assign a shared policy after you edit it. See:

[Assigning a policy to a group or location](#)

To edit a policy on the Policies page (Option 1)

1. To edit a policy on the Policies page, in the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the policy type.
3. In the **policy type Policies** pane, click the specific policy that you want to edit.
4. Under **Tasks**, click **Edit the Policy**.
5. In the **policy type Policy Overview** pane, edit the name and description of the policy, if necessary.
6. To edit the policy, click any of the **policy type Policy** pages for the policies.

To edit a policy on the Clients page (Option 2)

1. To edit a policy on the **Clients** page, in the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to edit a policy.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot edit a policy.
4. Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to edit.
5. Locate the specific policy for the location that you want to edit.
6. To the right of the selected policy, click **Tasks**, and then click **Edit Policy**.
7. Do one of the following tasks:
 - To edit a non-shared policy, go to the next step.
 - To edit a shared policy, in the **Edit Policy** dialog box, click **Edit Shared** to edit the policy in all locations.
8. You can click a link for the type of policy that you want to edit.

Finding a policy's default settings

If you have changed a policy's settings, you can return the policy to its default settings. You add a new policy of *<policy type>*, which includes the default settings automatically. See:

[Creating a custom Symantec Endpoint Protection Manager policy](#)

Copying and pasting a policy on the Policies page

You can copy and paste a policy on the **Policies** page. For example, you may want to edit the policy settings slightly to apply to another group.

To copy a policy in the Policies page

1. In the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to copy.
3. In the **policy type Policies** pane, click the specific policy that you want to copy.
4. On the **Policies** page, under **Tasks**, click **Copy the Policy**.
5. In the **Copy Policy** dialog box, check **Do not show this message again** if you no longer want to be notified about this process.
To redisplay the **Do not show this message again** check box, click **Admin > Administrators**, select your administrator account, and click **Reset Copy Policy Reminder**.
6. Click **OK**.

To paste a policy in the Policies page

1. In the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to paste.
3. In the **policy type Policies** pane, click the specific policy that you want to paste.
4. On the **Policies** page, under **Tasks**, click **Paste a Policy**.

More information

- [Copying and pasting a policy on the Clients page](#)
- [Performing the tasks that are common to all policies](#)

Copying and pasting a policy on the Clients page

You can copy and paste a policy instead of having to add a new policy. You can copy a shared or a non-shared policy on the **Clients** page.

To copy a policy in the Clients page

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to copy a policy.
3. On the **Policies** tab, under **Location-specific Policies and Settings**, scroll to find the name of the location from which you want to copy a policy.
4. Locate the specific policy for the location that you want to copy.
5. To the right of the policy, click **Tasks**, and then click **Copy**.
6. Click **OK**.

To paste a policy on the Clients page

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to paste a policy.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot paste a policy.
4. Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to paste.
5. Locate the specific policy for the location that you want to paste.
6. To the right of the policy, click **Tasks**, and then click **Paste**.

7. When you are prompted to overwrite the existing policy, click **Yes**.

More information

- [Copying and pasting a policy on the Policies page](#)
- [Performing the tasks that are common to all policies](#)

Assigning a policy to a group or location

You assign a policy to a client computer through a group. Every group has exactly one policy of each protection type that is assigned to it at all times. Typically, you create separate groups for the clients that run different platforms. If you put the clients that run different platforms into the same group, each client platform ignores any settings that do not apply to it.

Unassigned policies are not downloaded to the client computers in groups and locations. If you do not assign the policy when you add the policy, you can assign it to groups and locations later. You can also reassign a policy to a different group or location.

Policies are assigned to computer groups as follows:

- At initial installation, the Symantec default security policies are assigned to the **My Company** parent group.
- The security policies in the **My Company** parent group are automatically assigned to each newly created child group. Newly created child groups inherit from **My Company** by default.
New groups always inherit from their immediate parent group. If you create a hierarchy of child groups, each one inherits from its immediate parent, not from the top-level parent.
- You replace a policy in a group by assigning another policy of the same type. You can replace a policy that is assigned to the **My Company** parent group or to any child group.

The icons display the following information:

Table 69: Policy icons

Icon	Description
	A group without a policy that is assigned to it.
	A group with a policy assigned to it. The text is bold.
	A location without a policy that is assigned to it.
	A location with a policy assigned to it. The text is bold.
	A location that inherits from a parent group and has no policy that is assigned to it.
	A location that inherits from a parent group and has a policy that is assigned to it

To assign a policy to a group or location

1. In the console, click **Policies** > policy type.
2. On the **Policies** page, select a policy, and then click **Assign the policy**.
3. In the **Assign policy** dialog box, select the groups or locations, and then click **Assign**.
4. Click **OK** to confirm.

More information

Replacing a policy

You may want to replace one shared policy with another shared policy. You can replace the shared policy in either all locations or for individual locations.

When you replace a policy for all locations, the management server replaces the policy only for the locations that have it. For example, suppose the Sales group uses the Sales policy for three of its four locations. If you replace the Sales policy with the Marketing policy, only those three locations receive the Marketing policy.

You may want a group of clients to use the same settings no matter what location they are in. In this case, you can replace a non-shared policy with a shared policy. You replace a non-shared policy with a shared policy for each location individually.

To replace a shared policy for all locations

1. In the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to replace.
3. In the **policy type Policies** pane, click the policy.
4. In the **Policies** page, under **Tasks**, click **Replace the Policy**.
5. In the **Replace policy type Policy** dialog box, in the **New policy type Policy** list box, select the shared policy that replaces the old one.
6. Select the groups and locations for which you want to replace the existing policy.
7. Click **Replace**.
8. When you are prompted to confirm the replacement of the policy for the groups and locations, click **Yes**.

To replace a shared policy or non-shared policy for one location

1. In the console, click **Clients**.
2. In the **Clients** page, under **Clients**, select the group for which you want to replace a policy.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
4. Under **Location-specific Policies and Settings**, scroll to find the location that contains the policy.
5. Next to the policy that you want to replace, click **Tasks**, and then click **Replace Policy**.
6. In the **Replace Policy** dialog box, in the **New policy** list box, select the replacement policy.
7. Click **OK**.

More information

[Performing the tasks that are common to all policies](#)

Exporting and importing individual Endpoint Protection policies

You can export and import policies rather than recreating the policies. All the settings that are associated with the policy are automatically exported.

You may need to export a policy for the following reasons:

- You update the management server from an older release to a newer release. You want to update the new management server with the policies that you previously customized.
- You want to export a policy for use at a different site.

You export and import each policy one at a time. Once you export a file, you import it and apply it to a group or only to a location. You can export a shared or non-shared policy for a specific location in the **Clients** page.

To export a single policy from the Policies page

1. In the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to export.
3. In the **policy type Policies** pane, click the specific policy that you want to export.
4. In the **Policies** page, under **Tasks**, click **Export the Policy**.
5. In the **Export Policy** dialog box, locate the folder where you want to export the policy file to, and then click **Export**.

To export a shared or non-shared policy from the Clients page

1. In the console, click **Clients**.
2. Under **Clients**, select the group for which you want to export a policy.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot export a policy.
4. Under **Location-specific Policies and Settings**, scroll to find the name of the location whose policy you want to export.
5. Locate the specific policy for the location that you want to export.
6. To the right of the policy, click **Tasks**, and then click **Export Policy**.
7. In the **Export Policy** dialog box, browse to the folder into which you want to export the policy.
8. In the **Export Policy** dialog box, click **Export**.

To import a single policy

1. In the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to import.
3. In the **policy type Policies** pane, click the policy that you want to import.
4. On the **Policies** page, under **Tasks**, click **Import a policy type Policy**.
5. In the **Import Policy** dialog box, browse to the policy file that you want to import, and then click **Import**.

More information

[Performing the tasks that are common to all policies](#)

About shared and non-shared policies

Policies are either shared or non-shared. A policy is shared if you apply it to more than one group or location. If you create shared policies, you can easily edit and replace a policy in all groups and locations that use it. You can apply shared policies at the My Company group level or a lower group level and subgroups can inherit policies. You can have multiple shared policies.

If you need a specialized policy for a particular group or location, you create a policy that is unique. You assign this unique, non-shared policy to one specific group or location. You can only have one policy of each policy type per location.

For example, here are some possible scenarios:

- A group of users in Finance needs to connect to an enterprise network by using different locations when at the office and for home. You may need to apply a different Firewall policy with its own set of rules and settings to each location for that one group.
- You have remote users who typically use DSL and ISDN, for which they may need a VPN connection. You have other remote users who want to dial up when they connect to the enterprise network. However, the sales and marketing groups also want to use wireless connections. Each of these groups may need its own Firewall policy for the locations from which they connect to the enterprise network.
- You want to implement a restrictive policy regarding the installation of non-certified applications on most employee workstations to protect the enterprise network from attacks. Your IT group may require access to additional

applications. Therefore, the IT group may need a less restrictive security policy than typical employees. In this case, you can create a different Firewall policy for the IT group.

You typically add any policy that groups and locations share in the **Policies** page on the **Policies** tab. However, you add any policy that is not shared between groups and that applies only to a specific location in the **Clients** page. If you decide to add a policy in the **Clients** page, you can add a new policy by using any of the following methods:

- Add a new policy. See:
[Adding a policy](#)
- Copy an existing policy to base the new policy on. See:
 - [Copying and pasting a policy on the Policies page](#)
 - [Copying and pasting a policy on the Clients page](#)
- Import a policy that was previously exported from another site. See:
[Exporting and importing individual Endpoint Protection policies](#)

More information

- [Performing the tasks that are common to all policies](#)
- [Converting a shared policy to a non-shared policy](#)

Converting a shared policy to a non-shared policy

You can copy the content of a shared policy and create a non-shared policy from that content. A copy enables you to change the content of a shared policy in one location and not in all other locations. The copy overrides the existing shared policy.

When you finish the conversion, the converted policy with its new name appears under **Location-specific Policies and Settings**. However, the non-shared policy does not appear in the **Policies** page for the policy type unless you copy it from the **Clients** page > **Policies** tab to the **Policies** page.

For more information, see:

- [About shared and non-shared policies](#)
- [Copying and pasting a policy on the Clients page](#)
- [Copying and pasting a policy on the Policies page](#)

To convert a shared policy to a non-shared policy

1. In the console, click **Clients**.
2. In the **Clients** page, under **Clients**, select the group for which you want to convert a policy.
3. In the pane that is associated with the group that you selected in the previous step, click **Policies**.
4. On the **Policies** tab, uncheck **Inherit policies and settings from parent group group_name**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot replace a policy.
5. Under **Location-specific Policies and Settings**, scroll to find the name of the location and the specific policy that you want to convert.
6. Beside the specific policy, click **Tasks**, and then click **Convert to Non-shared Policy**.
7. In the **Overview** dialog box, edit the name and description of the policy.
8. Modify the other policy settings as desired.
9. Click **OK**.

More information

Unassigning a policy from a group or location

You may want to unassign a policy from a group or a location if you want to delete the policy permanently or save the policy to use for a later time.

For example, a specific group may have experienced problems after you introduced a new policy. If you want the policy to remain in the database, you can withdraw the policy instead of deleting it. If you withdraw a policy, it is automatically withdrawn from the groups and locations that you assigned it to. The number of locations that a policy is used for appears on the **policy type Policies** pane on the **Policies** page.

NOTE

You must withdraw a policy or replace a policy from all groups and locations before you can delete it.

You can withdraw all policies in the **Policies** page from a location or group except for the following policies:

- **Virus and Spyware Protection**
- **LiveUpdate Settings**

You can only replace them with another **Virus and Spyware Protection policy** or **LiveUpdate policy**. See:

- [Replacing a policy](#)
- [Assigning a policy to a group or location](#)

To unassign a shared policy in the Policies page

1. In the console, click **Policies**.
2. On the **Policies** page, under **Policies**, click the type of policy that you want to withdraw.
3. In the **policy type Policies** pane, click the specific policy that you want to withdraw.
4. On the **Policies** page, under **Tasks**, click **Withdraw the Policy**.
5. In the **Withdraw Policy** dialog box, check the groups and locations from which you want to withdraw the policy.
6. Click **Withdraw**.
7. When you are prompted to confirm the withdrawal of the policy from the groups and locations, click **Yes**.

To unassign a shared or non-shared policy in the Clients page

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to withdraw a policy.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
You must disable inheritance for this group. If you do not uncheck inheritance, you cannot withdraw a policy.
4. Under **Location-specific Policies and Settings**, scroll to find the name of the location for which you want to withdraw a policy.
5. Locate the policy for the location that you want to withdraw.
6. Click **Tasks**, and then click **Withdraw Policy**.
7. In the **Withdraw Policy** dialog box, click **Yes**.

More information

Enabling application learning

You may want to monitor and collect information about the applications and services that run on each computer in your environment.

You use this information to add to the following policies and features:

-
- Firewall policies
 - Application and Device Control policies
 - Behavioral analysis
 - Host Integrity policies
 - Network application monitoring
 - File fingerprint lists

You configure the client to collect the information and then send the list to the management server. The more clients there are, the larger variety of applications and data is temporarily stored. This data can generate CPU or memory issues for already under-resourced management servers. As a best practice, run application learning on a subset of clients first.

NOTE

In some countries, it may not be permissible under the local law to use the learned applications tool under certain circumstances. For example, you may want to gather a list of applications that employees access from their company laptops when they log on to your office network versus from their home. Before you use this tool, confirm that you can use the tool in your jurisdiction. If it is not permitted, keep application learning disabled.

NOTE

The Mac and Linux clients do not support learned applications.

Step 1: Enabling application learning for a site

To enable application learning for a site

1. In the console, click **Admin > Servers**.
2. Under View Servers, do one of the following actions:
 - a. Click **Local Site (Site <site name>)**.
 - b. Expand **Remote Sites**, and then click **Site <site name>**.
3. Under **Tasks**, click **Edit Site Properties**.
4. On the **General** tab, check **Keep track of every application that the clients run**.
5. To minimize the database space that is taken up by learned application data, check **Delete learned application data after x days**. If you have trouble updating the management server database, Symantec recommends you enter 7.
6. Click **OK**.

Step 2: Send learned applications to the management server for a location or a group

After you have enabled a site to collect the lists of learned applications from the clients, you enable the clients to send the lists to the server by group or by location.

NOTE

The client must have the Network Threat Protection component installed for this feature to work.

To send learned applications to the management server for a group

1. In the console, click **Clients**, select a group, and then click **Policies**.
2. On the **Policies** tab, click **Communications Settings**.
3. In the **Communications Settings** dialog box, check **Learn applications that run on the client computers**, and then click **OK**.

To send learned applications to the management server for a location

1. In the console, click **Clients**, select a group, and then click **Policies**.
2. On the **Policies** tab, select the location, and then expand **Location-specific Settings**.
3. To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings** and click **Edit Settings**.

Checking this setting enables you to create a location setting rather than a group setting.

-
4. In the **Communications Settings for location name** dialog box, check **Learn applications that run on the client computers**, and then click **OK**

More information:

- To allow changes in the application checksum, you must enable Network Application Monitoring. See: [Blocking networked applications that might be under attack](#)
- You can set up a notification to be sent to your email address when each client in a group or location runs an application. See: [Setting up administrator notifications](#)
- [Creating an application exception](#)

Searching for information about the learned applications that the computers run

After the management server receives the list of learned applications from the clients, you can run queries to find out details about the applications. For example, you can find all the client computers that use an unauthorized application. You can then create a firewall rule to block the application on the client computer. Or you may want to upgrade all the client computers to use the most current version of Microsoft Word. You can use the **Search for Applications** task from any type of policy.

NOTE

The Mac client does not monitor the applications and the services.

You can search for an application in the following ways:

- By application.
You can limit the search to specific applications or application details such as its name, file fingerprint, path, size, version, or last modified time.
- By client or client computer.
You can search for the applications that either a specific user runs or a specific computer runs. For example, you can search on the computer's IP address.

You can also search for application names to add to a firewall rule, directly within the Firewall policy. See:

[Defining information about applications](#)

NOTE

The information in the **Search** box is not collected until you enable the feature that keeps track of all the applications that clients run. You can go to the **Clients** page, **Communications Settings** dialog box for each group or location to enable this feature.

To search for information about the applications that the computers run

1. In the console, click **Policies**.
2. On the **Policies** page, under **Tasks**, click **Search for Applications**.
3. In the **Search for Applications** dialog box, to the right of the **Search for applications in** field, click **Browse**.
4. In the **Select Group or Location** dialog box, select a group of clients for which you want to view the applications, and then click **OK**.

You can specify only one group at a time.

5. Make sure that **Search subgroups** is checked.
6. Do one of the following actions:
 - To search by user or computer information, click **Based on client/computer information**.
 - To search by application, click **Based on applications**.

7. Click the empty cell under **Search Field**, and then select the search criterion from the list.
The Search Field cell displays the criteria for the option that you selected. For details about these criteria, click **Help**.
8. Click the empty cell under Comparison Operator, and then select one of the operators.
9. Click the empty cell under Value, and then select or type a value.
The Value cell may provide a format or a value from the drop-down list, depending on the criterion you selected in the Search Field cell.
10. To add an additional search criterion, click the second row, and then enter information in the Search Field, Comparison Operator, and Value cells.
If you enter more than one row of search criteria, the query tries to match all conditions.
11. Click **Search**.
12. In the Query Results table, do any of the following tasks:
 - Click the scroll arrows to view additional rows and columns.
 - Click **Previous** and **Next** to see additional screens of information.
 - Select a row, and then click **View Details** to see additional information about the application.
 The results are not saved unless you export them to a file.
13. To remove the query results, click **Clear All**.
14. Click **Close**.

More information

- [Performing the tasks that are common to all policies](#)

Managing firewall protection

The firewall allows the incoming network traffic and outgoing network traffic that you specify in the firewall policy. The Symantec Endpoint Protection firewall policy contains rules and protection settings, most of which you can enable or disable and configure.

Table 70: Optional tasks to manage firewall protection

Task	Description
Read about firewall protection	Before you configure your firewall protection, you should familiarize yourself with the firewall. See: • How a firewall works • About the Symantec Endpoint Protection firewall
Modify the existing default firewall policy or create a new policy	You can modify the default policy or create new ones. See: Creating a firewall policy
Create and customize firewall rules	Firewall rules are the policy components that control how the firewall protects client computers from malicious attacks. The default firewall policy contains default firewall rules. And when you create a new policy, Symantec Endpoint Protection provides default firewall rules. However, you can modify the default rules or create new ones. See: • Adding a new firewall rule • Customizing firewall rules

Task	Description
Enable firewall protection settings	After the firewall has completed certain operations, control is passed to a number of components. Each component is designed to perform a different type of packet analysis. See: • Enabling communications for network services instead of adding a rule • Automatically blocking connections to an attacking computer • Preventing outside stealth attacks on computers • Disabling the Windows Firewall • Blocking a remote computer by configuring peer-to-peer authentication
Monitor firewall protection	Regularly monitor the firewall protection status on your computers. See: Monitoring the Symantec Endpoint Protection clients

More information

- [Running commands on client computers from the console](#)
- [Configuring firewall settings for mixed control](#)

How a firewall works

A firewall prevents any unauthorized users from accessing the computers and networks in your organization that connect to the Internet.

In addition, a firewall performs the following tasks:

- Monitors the communication between your computers and other computers on the Internet
- Creates a shield that allows or blocks attempts to access the information on your computer
- Warns you of connection attempts from other computers
- Warns you of connection attempts by the applications on your computer that connect to other computers

The firewall reviews the packets of data that travel across the Internet. A packet is a discrete unit of data that is part of the information flow between two computers. Packets are reassembled at their destination to appear as an unbroken data stream.

Packets include the following information about the data:

- The originating computer
- The intended recipient or recipients
- How the packet data is processed
- Ports that receive the packets

Ports are the channels that divide the stream of data that comes from the Internet. Applications that run on a computer listen to the ports. The applications accept the data that is sent to the ports.

Network attacks exploit weaknesses in vulnerable applications. Attackers use these weaknesses to send the packets that contain malicious programming code to ports. When vulnerable applications listen to the ports, the malicious code lets the attackers gain access to the computer.

About the Symantec Endpoint Protection firewall

The Symantec Endpoint Protection firewall uses firewall policies and rules to allow or block network traffic. The Symantec Endpoint Protection includes a default Firewall policy with default firewall rules and firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

Firewall rules control how the client protects the client computer from malicious inbound traffic and malicious outbound traffic. The firewall automatically checks all the inbound and the outbound packets against these rules. The firewall then

allows or blocks the packets based on the information that is specified in rules. When a computer tries to connect to another computer, the firewall compares the type of connection with its list of firewall rules. The firewall also uses stateful inspection of all network traffic.

When you install the console for the first time, it adds a default Firewall policy to each group automatically.

Every time you add a new location, the console copies a Firewall policy to the default location automatically.

You determine the level of interaction that you want users to have with the client by permitting or blocking their ability to configure firewall rules and firewall settings. Users can interact with the client only when it notifies them of new network connections and possible problems. Or they can have full access to the user interface.

You can install the client with default firewall settings. In most cases you do not have to change the settings. However, if you have a detailed understanding of networks, you can make many changes in the client firewall to fine-tune the client computer's protection.

As of version 14.2, the Mac client offers a firewall for the managed client only. The user can only enable or disable the firewall if the administrator has allowed client control. Since it operates on a different network layer than the Mac's operating system firewall, they can both be enabled and run in parallel.

More information

- [About firewall settings for the Mac client](#)
- [Managing firewall protection](#)
- [How a firewall works](#)
- [How the firewall uses stateful inspection](#)
- [The types of security policies](#)

Creating a firewall policy

The Symantec Endpoint Protection includes a default Firewall policy with default firewall rules and default firewall settings for the office environment. The office environment is normally under the protection of corporate firewalls, boundary packet filters, or antivirus servers. Therefore, it is normally more secure than most home environments, where limited boundary protection is available.

When you install the console for the first time, it adds a default Firewall policy to each group automatically.

NOTE

Changing the name of the default Firewall policy may result in an upgrade not updating the policy. The same applies to the default rules within the default Firewall policy.

Every time you add a new location, the console copies a Firewall policy to the default location automatically. If the default protection is not appropriate, you can customize the Firewall policy for each location, such as for a home site or customer site. If you do not want the default Firewall policy, you can edit it or replace it with another shared policy.

The following table describes the tasks that you can perform to configure a new firewall policy. You must add a firewall policy first, but thereafter, the remaining tasks are optional and you can complete them in any order.

Table 71: How to create a firewall policy

Task	Description
Add new firewall rules	Firewall rules are the policy components that control how the firewall protects client computers from malicious incoming traffic and applications. The firewall automatically checks all incoming packets and outgoing packets against these rules. It allows or blocks the packets based on the information that is specified in rules. You can modify the default rules, create new rules, or disable the default rules. When you create a new Firewall policy, Symantec Endpoint Protection provides default firewall rules that are enabled by default. For more information, see: Adding a new firewall rule
Enable and customize notifications to users that access to an application is blocked	You can send users a notification that an application that they want to access is blocked. These settings are disabled by default. For more information, see: Notifying the users that access to an application is blocked
Enable automatic firewall rules	You can enable the options that automatically permit communication between certain network services. These options eliminate the need to create the rules that explicitly allow those services. You can also enable traffic settings to detect and block the traffic that communicates through NetBIOS and token rings. Only the traffic protocols are enabled by default. For more information, see: Enabling communications for network services instead of adding a rule If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an Active Response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location. This option is disabled by default. For more information, see: Automatically blocking connections to an attacking computer
Configure protection and stealth settings	You can enable settings to detect and log potential attacks on the client and block spoofing attempts. You can enable the settings that prevent outside attacks from detecting information about your clients. For more information, see: Preventing outside stealth attacks on computers All of the protection options and stealth options are disabled by default.
Integrate the Symantec Endpoint Protection firewall with the Windows firewall	You can specify the conditions in which Symantec Endpoint Protection disables the Windows firewall. When Symantec Endpoint Protection is uninstalled, Symantec Endpoint Protection restores the Windows firewall setting to the state it was in before Symantec Endpoint Protection was installed. The default setting is to disable the Windows firewall once only and to disable the Windows firewall disabled message. For more information, see: Disabling the Windows Firewall
Configure peer-to-peer authentication	You can use peer-to-peer authentication to allow a remote client computer (peer) to connect to another client computer (authenticator) within the same corporate network. The authenticator temporarily blocks inbound TCP and UDP traffic from the remote computer until the remote computer passes the Host Integrity check. This option is disabled by default. For more information, see: Blocking a remote computer by configuring peer-to-peer authentication

When you enable firewall protection, the policy allows all inbound IP-based network traffic and all outbound IP-based network traffic, with the following exceptions:

- The default firewall protection blocks inbound and outbound IPv6 traffic with all remote systems.

NOTE

IPv6 is a network layer protocol that is used on the Internet. If you install the client on the computers that run Microsoft Vista, the **Rules** list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

- The default firewall protection restricts the inbound connections for a few protocols that are often used in attacks (for example, Windows file sharing).

Internal network connections are allowed and external networks are blocked.

[Managing firewall protection](#)

[Best practices for Firewall policy settings for remote clients](#)

Managing firewall rules from the Symantec Endpoint Protection Manager

Firewall rules control how the firewall protects computers from malicious incoming traffic and applications. The firewall checks all incoming packets and outgoing packets against the rules that you enable. It allows or blocks the packets based on the conditions that you specify in the firewall rule.

Symantec Endpoint Protection installs with a default firewall policy that contains default rules. When you create a new firewall policy, Symantec Endpoint Protection provides default firewall rules. You can modify any of the default rules or create new firewall rules if your administrator permits it, or if your client is unmanaged.

You must have at least one rule in a policy. But you can have as many rules as you need. You can enable or disable rules as needed. For example, you might want to disable a rule to perform troubleshooting and enable it when you are done.

The following table describes what you need to know to manage firewall rules.

Table 72: Managing firewall rules

Task	Description
Learn how firewall rules work and what makes up a firewall rule	Before you modify the firewall rules, you should understand how firewall rules work: • How to order rules to ensure that the most restrictive rules are evaluated first and the most general rules are evaluated last. See: About the firewall rule, firewall setting, and intrusion prevention processing order • That the client uses stateful inspection, which keeps track of the state of the network connections. See: How the firewall uses stateful inspection • The firewall components that make up the firewall rule. When you understand about these triggers and how you can best use them, you can customize your firewall rules to protect your clients and servers.
Add a new firewall rule	You can perform the following tasks to manage firewall rules: • Add new firewall rules through the console using several methods. One method lets you add a blank rule that has default settings. The other method offers a wizard that guides you through creating a new rule. • Customize a rule by changing any of the firewall rule criteria. • Export and import firewall rules from another firewall policy. • Copy and paste firewall rules. You can save time creating a new firewall rule by copying an existing rule that is similar to the rule that you want to create. Then you can modify the copied rule to meet your needs.

Task	Description
Customize a firewall rule	After you create a new rule, or if you want to customize a default rule, you can modify any of the firewall rule criteria.

Adding a new firewall rule

You can create new firewall rules using either of the following methods:

Blank rule	A blank rule allows all traffic. See: To add a new blank firewall rule
Add Firewall Rule wizard	If you add rules with the Add Firewall Rule wizard, ensure that you configure the rule. The wizard does not configure new rules with multiple criteria. See; To add a firewall rule using a wizard

You should specify both the inbound and the outbound traffic in the rule whenever possible. You do not need to create inbound rules for traffic such as HTTP. The Symantec Endpoint Protection client uses stateful inspection for TCP traffic. Therefore, it does not need a rule to filter the return traffic that the clients initiate.

When you create a new firewall rule, it is automatically enabled. You can disable a firewall rule if you need to allow specific access to a computer or application. The rule is disabled for all inherited policies.

The rule is also disabled for the all locations if it is a shared policy and only one location if it is a location-specific policy.

NOTE

Rules must be enabled for the firewall to process them.

To add a new blank firewall rule

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.
3. On the **Rules** tab, under the **Rules** list, click **Add Blank Rule**.
4. Optionally, you can change the firewall rule criteria as needed.
5. If you are done with the configuration of the rule, click **OK**.

To add a firewall rule using a wizard

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.
3. Fill out the options on each screen, and then click **Next**.
4. Click **Finish**.
Optionally, you can change the firewall rule criteria as needed.

More information

- [Customizing firewall rules](#)
- [How the firewall uses stateful inspection](#)

About firewall server rules and client rules

Rules are categorized as either server rules or client rules. Server rules are the rules that you create in Symantec Endpoint Protection Manager and that are downloaded to the Symantec Endpoint Protection client. Client rules are the rules that the user creates on the client.

All rules on the Mac client are server rules. Mac users do not have the option of creating client rules for the Mac client.

The firewall was introduced in the Mac client as of version 14.2.

The following table describes the relationship between the client's user control level and the user's interaction with the firewall rules.

Table 73: User control level and rule status

User control level	User interaction
Server control	The Windows client receives server rules but the user cannot view them. The user cannot create client rules. The Mac client does not allow the user to enable or disable the firewall.
Mixed control	The Windows client receives server rules. The user can create client rules, which are merged with server rules and client security settings. The Mac client allows or disallows the user to enable or disable the firewall. It depends on whether the granular setting is set to server control or client control.
Client control	The client does not receive server rules. The user can create client rules. The Symantec Endpoint Protection Manager administrator cannot view client rules. The Mac client allows the user to enable or disable the firewall.

For more information, see:

[Preventing users from disabling protection on client computers](#)

The following table lists the order that the firewall processes server rules, client rules, and client settings.

Table 74: Server rules and client rules processing priority

Priority	Rule type or setting
First	Server rules with high priority levels (rules above the blue line in the Rules list)
Second	Client rules
Third	Server rules with lower priority levels (rules under the blue line in the Rules list) On the client, server rules under the blue line are processed after client rules.
Fourth	Client security settings
Fifth	Client application-specific settings

On the client, users can modify a client rule or security setting, but users cannot modify a server rule.

WARNING

If the client is in mixed control, users can create a client rule that allows all traffic. This rule overrides all server rules under the blue line.

More information

- [Managing firewall rules](#)
- [Changing the order of firewall rules](#)
- [Preventing users from disabling protection on client computers](#)

What is the order that the firewall processes the firewall rules and settings

Firewall rules are ordered sequentially, from highest to lowest priority in the rules list. If the first rule does not specify how to handle a packet, the firewall inspects the second rule.

This process continues until the firewall finds a match. After the firewall finds a match, the firewall takes the action that the rule specifies. Subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

You can order rules according to exclusivity. The most restrictive rules are evaluated first, and the most general rules are evaluated last.

The following table displays the best practices for ordering firewall rules.

1st	Rules that block all traffic.
2nd	Rules that allow all traffic.
3rd	Rules that allow or block specific computers.
4th	Rules that allow or block specific applications, network services, and ports.

In the Symantec Endpoint Protection Manager, the Rules list contains a blue dividing line. The dividing line sets the priority of rules in the following situations:

- When a subgroup inherits rules from a parent group.
- When the Windows client is set to mixed control. The firewall processes both server rules and client rules.

The following table shows the order in which the firewall processes the rules, firewall settings, and intrusion prevention settings.

Table 75: Processing order

Priority	Setting
1	Custom IPS signatures
2	IPS settings and protection and stealth settings, except for port scans
3	Built-in rules
4	Firewall rules
5	Port scan checks
6	IPS signatures that are downloaded through LiveUpdate

About inherited firewall rules

A subgroup's policy can inherit only the firewall rules that are enabled in the parent group. When you have inherited the rules, you can disable them, but you cannot modify them. As the new rules are added to the parent group's policy, the new rules are automatically added to the inheriting policy.

When the inherited rules appear in the **Rules** list, they are shaded in italics. Above the blue line, the inherited rules are added above the rules that you created as Symantec Endpoint Protection Manager administrator. Below the blue line, the inherited rules are added below the rules that you created.

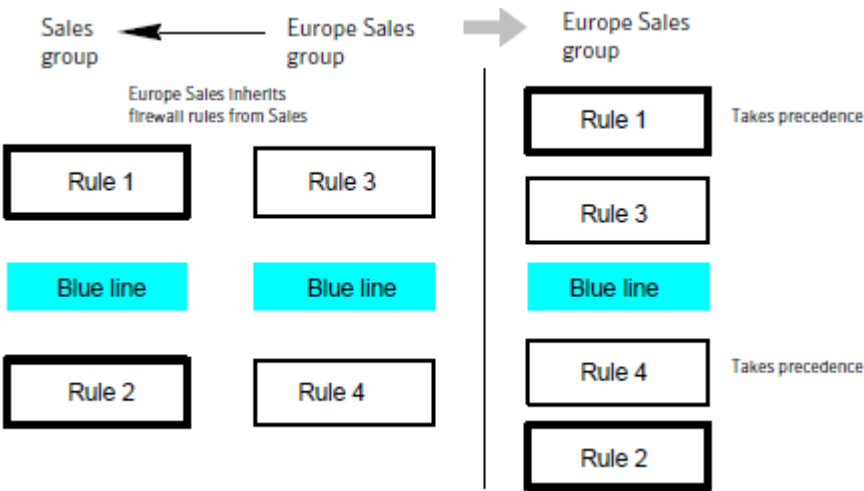
A Firewall policy also inherits default rules, so the subgroup's Firewall policy may have two sets of default rules. You may want to delete one set of default rules.

If you want to remove the inherited rules, you remove the inheritance rather than delete them. You have to remove all the inherited rules rather than the selected rules.

The firewall processes inherited firewall rules in the **Rules** list as follows:

Above the blue dividing line	The rules that the policy inherits take precedence over the rules that you create.
Below the blue dividing line	The rules that you create take precedence over the rules that the policy inherits.

The following figure shows how the **Rules** list orders rules when a subgroup inherits rules from a parent group. In this example, the Sales group is the parent group. The Europe Sales group inherits from the Sales group.



More information

- [Managing firewall rules](#)
- [Adding inherited firewall rules from a parent group](#)

Adding inherited firewall rules from a parent group

You can add firewall rules to a firewall policy by inheriting rules from a parent group. To inherit the rules from a parent group, the subgroup's policy must be a non-shared policy.

NOTE

If the group inherits all of its policies from a parent group, this option is unavailable.

To add inherited firewall rules from a parent group

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.
For versions earlier than 14.2, there is no option for **Mac Settings**.
3. On the **Rules** tab, check **Inherit Firewall Rules from Parent Group**.
To remove the inherited rules, uncheck **Inherit Firewall Rules from Parent Group**.
4. Click **OK**.

More information

-
- [Editing a policy](#)
 - [About inherited firewall rules](#)
 - [Managing firewall rules](#)

Changing the order of firewall rules

The firewall processes the list of firewall rules from the top down. You can determine how the firewall processes firewall rules by changing their order.

If the Symantec Endpoint Protection client uses location switching, when you change the firewall rule order, the change affects the order for the current location only.

NOTE

For better protection, place the most restrictive rules first and the least restrictive rules last.

For more information, see:

[About the firewall rule, firewall setting, and intrusion prevention processing order](#)

To change the order of a firewall rule in the management server

1. In the console, open a Firewall policy.
2. In the **Firewall Policy** page, click **Rules**, and then select the rule that you want to move.
3. Do one of the following tasks:
 - To process this rule before the previous rule, click **Move Up**.
 - To process this rule after the rule below it, click **Move Down**.
4. Click **OK**.

To change the order of a firewall rule in the client

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options > Configure Firewall Rules**.
3. In the **Configure Firewall Rules** dialog box, select the rule that you want to move.
4. Do one of the following actions:
 - To have the firewall process this rule before the rule above it, click the up arrow.
 - To have the firewall process this rule after the rule below it, click the down arrow.
5. When you finish moving rules, click **OK**.

More information

[Managing firewall rules](#)

How the firewall uses stateful inspection

Firewall protection uses stateful inspection to track current connections. Stateful inspection tracks source and destination IP addresses, ports, applications, and other connection information. Before the client inspects the firewall rules, it makes the traffic flow decisions that are based on the connection information.

For example, if a firewall rule allows a computer to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the computer is expected. It permits the Web server traffic to flow to the initiating computer without inspecting the rule base. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection eliminates the need to create new rules. For the traffic that is initiated in one direction, you do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet

(port 23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; you create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic. Because the firewall is stateful in nature, you only need to create the rules that initiate a connection, not the characteristics of a particular packet. All packets that belong to an allowed connection are implicitly allowed as being an integral part of that same connection.

Stateful inspection supports all rules that direct TCP traffic.

Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, you must create the rules that permit the traffic in both directions. For example, for the clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

The state table that maintains the connection information may be periodically cleared. For example, it is cleared when a Firewall policy update is processed or if Symantec Endpoint Protection services are restarted.

About firewall rule application triggers

When the application is the only trigger you define in a rule that allows traffic, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and you define no other triggers. Users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.

Application-based rules may be difficult to troubleshoot because an application may use multiple protocols. For example, if the firewall processes a rule that allows Internet Explorer before a rule that blocks FTP, the user can still communicate with FTP. The user can enter an FTP-based URL in the browser, such as `ftp://ftp.symantec.com`.

For example, suppose you allow Internet Explorer and define no other triggers. Computer users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the network protocols and hosts with which communication is allowed.

You should not use application rules to control traffic at the network level. For example, a rule that blocks or limits the use of Internet Explorer would have no effect should the user use a different Web browser. The traffic that the other Web browser generates would be compared against all other rules except the Internet Explorer rule. Application-based rules are more effective when the rules are configured to block the applications that send and receive traffic.

More information

- [Defining information about applications](#)
- [Notifying the users that access to an application is blocked](#)
- [Managing firewall rules](#)
- [Blocking networked applications that might be under attack](#)

Defining information about applications

You can define information about the applications that clients run and include this information in a firewall rule.

You can define applications in the following ways:

- Type the information manually. See:
[To define information about applications manually](#)
- Search for the application in the learned applications list.
Applications in the learned applications list are the applications that client computers in your network run. See:
[To search for applications from the learned applications list](#)

To define information about applications manually

1. In the console, open a Firewall policy.
2. On the **Firewall Policies** page, under **Windows Settings**, click **Rules**.
For versions earlier than 14.2, on the **Firewall Policies** page, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, right-click the **Application** field for the rule you want to change, and then click **Edit**.
4. In the **Application List** dialog box, click **Add**.
5. In the **Add Application** dialog box, enter one or more of the following fields:
 - File name, which can include the file path
 - File description
This field is used for display purposes only. It does not function as a matching condition.
 - File size, in bytes
 - Date that the application was last changed
 - File fingerprint

NOTE

Network Application Monitoring must be enabled to define a firewall rule by file size, date last modified, or file fingerprint. If Network Application Monitoring is disabled, rule processing ignores all fields except for **File Name**.

6. Click **OK** to add the application conditions.
7. Click **OK** to save the application list.

To search for applications from the learned applications list

1. On the **Firewall Policies** page, click **Rules**.
2. On the **Rules** tab, select a rule, right-click the **Application** field, and then click **Edit**.
3. In the **Application List** dialog box, click **Add From**.
4. In the **Search for Applications** dialog box, search for an application.
5. Under the **Query Results** table, to add the application to the **Applications** list, select the application, click **Add**, and then click **OK**.
6. Click **Close**.
7. Click **OK**.

More information

- [Managing firewall rules](#)
- [Editing a policy](#)
- [About firewall rule application triggers](#)

Blocking networked applications that might be under attack

Network application monitoring tracks an application's behavior in the security log. If an application's content is modified too frequently, it is likely that a Trojan horse attacked the application and the client computer is not safe. If an application's content is modified on an infrequent basis, it is likely that a patch was installed and the client computer is safe. You can use this information to create a firewall rule that allows or blocks an application.

You can configure the client to detect and monitor any application that runs on the client computer and that is networked. Network applications send and receive traffic. The client detects whether an application's content changes.

If you suspect that a Trojan horse has attacked an application, you can use network application monitoring to configure the client to block the application. You can also configure the client to ask users whether to allow or block the application.

An application's content changes for the following reasons:

- A Trojan horse attacked the application.
- The application was updated with a new version or an update.

You can add applications to a list so that the client does not monitor them. You may want to exclude the applications that you think are safe from a Trojan horse attack, but that have frequent and automatic patch updates.

You may also want to minimize the number of notifications that ask users to allow or block a network application.

To block networked applications that might be under attack

1. In the console, click **Clients**.
2. Under **Clients**, select a group, and then click **Policies**.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, click **Network Application Monitoring**.
4. In the **Network Application Monitoring for group name** dialog box, click **Enable Network Application Monitoring**.
5. In the **When an application change is detected** drop-down list, select the action that the firewall takes on the application that runs on the client as follows:

Ask	Asks the user to allow or block the application.
Block the traffic	Blocks the application from running.
Allow and Log	Allows the application to run and records the information in the security log. The firewall takes this action on the applications that have been modified only.

6. If you selected **Ask**, click **Additional Text**.
7. In the **Additional Text** dialog box, type the text that you want to appear under the standard message, and then click **OK**.
8. To exclude an application from being monitored, under **Unmonitored Application List**, do one of the following tasks:

To define an application manually	Click Add , fill out one or more fields, and then click OK .
To define an application from a learned applications list	Click Add From . The learned applications list monitors both networked and non-networked applications. You must select networked applications only from the learned applications list. After you have added applications to the Unmonitored Applications List , you can enable, disable, edit, or delete them.

9. Check the box beside the application to enable it; uncheck it to disable it.
10. Click **OK**.

More information

- [Managing firewall rules](#)
- [Notifying the users that access to an application is blocked](#)
- [Enabling application learning](#)

Notifying the users that access to an application is blocked

You can send users a notification that an application that they want to access is blocked. This notification appears on the users' computers.

NOTE

Enabling too many notifications can not only overwhelm your users, but can also alarm them. Use caution when enabling notifications.

To notify the users that access to an application is blocked

1. In the console, open a Firewall policy.
2. On the **Firewall Policies** page, click **Rules**.
3. On the **Notifications** tab, check **Display notification on the computer when the client blocks an application** and optionally add a custom message.
4. Click **OK**.

More information

- [Managing firewall rules](#)
- [Configuring client notifications for intrusion prevention and Memory Exploit Mitigation](#)
- [Setting up administrator notifications](#)

About firewall rule host triggers

You specify the host on both sides of the described network connection when you define host triggers.

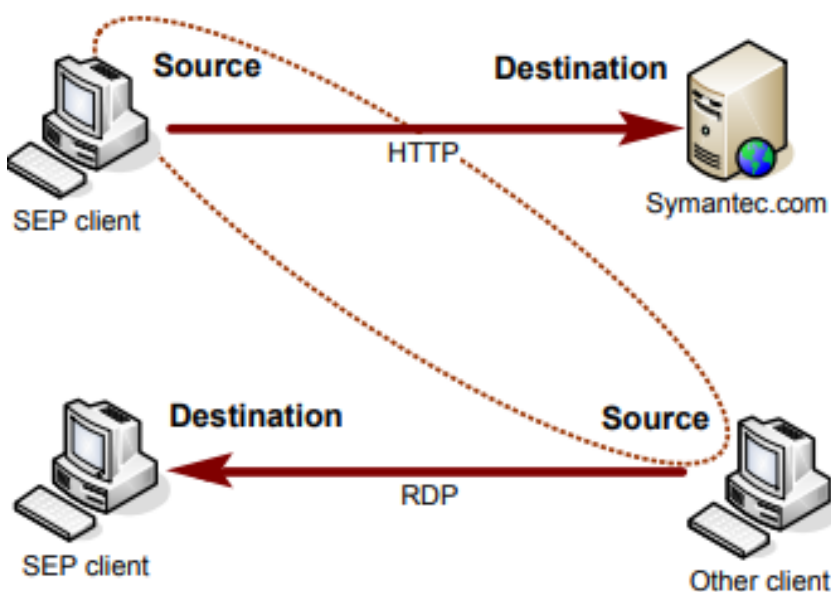
Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection.

You can define the host relationship in either one of the following ways:

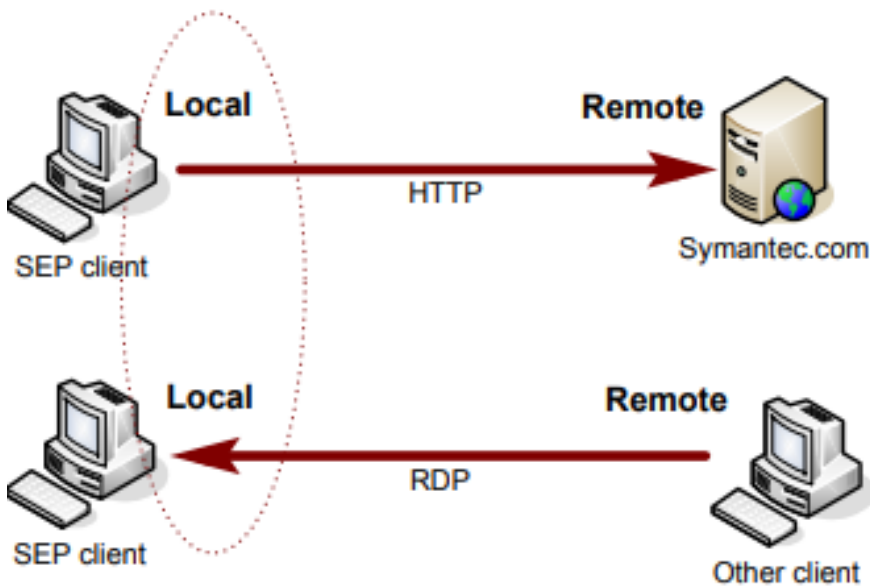
Source and destination	The source host and destination host are dependent on the direction of traffic. In one case the local client computer might be the source, whereas in another case the remote computer might be the source. The source and the destination relationship are more commonly used in network-based firewalls.
Local and remote	The local host is always the local client computer, and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic. The local and the remote relationship is more commonly used in host-based firewalls, and is a simpler way to look at traffic.

You can define multiple source hosts and multiple destination hosts.

The following diagram illustrates the source relationship and destination relationship with respect to the direction of traffic.



The following diagram illustrates the local host and remote host relationship with respect to the direction of traffic.



Relationships are evaluated by the following types of statements:

The hosts that you define on either side of the connection (between the source and the destination)	OR statement
Selected hosts	AND statement

For example, consider a rule that defines a single local host and multiple remote hosts. As the firewall examines the packets, the local host must match the relevant IP address. However, the opposing sides of the address may be matched to any remote host. For example, you can define a rule to allow HTTP communication between the local host and either Yahoo.com or Google.com. The single rule is the same as two rules.

More information

- [Adding host groups](#)
- [Blocking traffic to or from a specific server](#)
- [Managing firewall rules](#)

Adding host groups

A host group is a collection of: DNS domain names, DNS host names, IP addresses, IP ranges, MAC addresses, or subnets that are grouped under one name. The purpose of host groups is to eliminate the retyping of host addresses and names. For example, you can add multiple IP addresses one at a time to a firewall rule. Or, you can add multiple IP addresses to a host group, and then add the group to the firewall rule.

As you incorporate host groups, you must describe where the groups are used. If you decide later to delete a host group, you must first remove the host group from all the firewall rules that reference the group.

When you add a host group, it appears at the bottom of the **Hosts** list. You can access the **Hosts** list from the **Host** field in a firewall rule.

To add host groups

-
1. In the console, click **Policies**.
 2. Expand **Policy Components**, and then click **Host Groups**.
 3. Under **Tasks**, click **Add a Host Group**.
 4. In the **Host Group** dialog box, type a name, and then click **Add**.
 5. In the **Host** dialog box, in the **Type** drop-down list, select a host.
 6. Type the appropriate information for each host type.
 7. Click **OK**.
 8. Add additional hosts, if necessary.
 9. Click **OK**.

More information

[About firewall rule host triggers](#)

About firewall rule network services triggers

Network services let networked computers send and receive messages, share files, and print. A network service uses one or more protocols or ports to pass through a specific type of traffic. For example, the HTTP service uses ports 80 and 443 in the TCP protocol. You can create a firewall rule that allows or blocks network services. A network service trigger identifies one or more network protocols that are significant in relation to the described network traffic.

When you define TCP-based or UDP-based service triggers, you identify the ports on both sides of the described network connection. Traditionally, ports are referred to as being either the source or the destination of a network connection.

More information

- [Adding network services to the default network services list](#)
- [Permitting clients to browse for files and printers in the network](#)
- [Managing firewall rules](#)

Adding network services to the default network services list

Network services let networked computers send and receive messages, share files, and print. You can create a firewall rule that allows or blocks network services.

The network services list eliminates the need to retype protocols and ports for the firewall rules that you create to block or allow network services. When you create a firewall rule, you can select a network service from a default list of commonly used network services. You can also add network services to the default list. However, you need to be familiar with the type of protocol and the ports that it uses.

NOTE

IPv4 and IPv6 are the two network layer protocols that are used on the Internet. If you install the client on the computers that run Windows Vista, the **Rules** list includes several default rules that block the Ethernet protocol type of IPv6. If you remove the default rules, you must create a rule that blocks IPv6.

NOTE

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom network service from any other rule.

To add network services to the default network services list

-
1. In the console, click **Policies**.
 2. Expand **Policy Components**, and then click **Network Services**.
 3. Under **Tasks**, click **Add a Network Service**.
 4. In the **Network Service** dialog box, type a name for the service, and then click **Add**.
 5. Select a protocol from the **Protocol** drop-down list.
The options change based on which protocol you select.
 6. Type in the appropriate fields, and then click **OK**.
 7. Add one or more additional protocols, as necessary.
 8. Click **OK**.

More information

- [Managing firewall rules](#)
- [About firewall rule network services triggers](#)
- [Controlling whether networked computers can share messages, files, and printing](#)
- [Permitting clients to browse for files and printers in the network](#)

About firewall rule network adapter triggers

You can define a firewall rule that blocks or allows traffic that passes through (transmitted or received) a network adapter.

When you define a particular type of adapter, consider how that adapter is used. For example, if a rule allows outbound HTTP traffic from Ethernet adapters, then HTTP is allowed through all the installed adapters of the same type. The only exception is if you also specify local host addresses. The client computer may use multi-NIC servers and the workstations that bridge two or more network segments. To control traffic relative to a particular adapter, the address scheme of each segment must be used rather than the adapter itself.

The network adapter list eliminates the need to retype types of adapters for firewall rules. Instead, when you create a firewall rule, you can select a network adapter from a default list of commonly used network adapters. You can also add network adapters to the default list.

You can select a network adapter from a default list that is shared across firewall policies and rules. The most common adapters are included in the default list in the **Policy Components** list.

NOTE

You can add a custom network adapter through a firewall rule. However, that network adapter is not added to the default list. You cannot access the custom network adapter from any other rule.

More information

- [Managing firewall rules](#)
- [Adding a custom network adapter to the network adapter list](#)
- [Controlling the traffic that passes through a network adapter](#)

Adding a custom network adapter to the network adapter list

You can apply a separate firewall rule to each network adapter. For example, you may want to block traffic through a VPN at an office location, but not at a home location.

You can select a network adapter from a default list that is shared across firewall policies and rules. The most common adapters are included in the default list in the **Policy Components** list. Use the default list so that you do not have to retype each network adapter for every rule that you create.

The network adapter list eliminates the need to retype adapters for firewall rules. When you create a firewall rule, you can select a network adapter from a default list of commonly used network adapters. You can also add network adapters to the default list.

NOTE

You can add a custom network adapter through a firewall rule. However, that network adapter is not added to the default list. You cannot access the custom network adapter from any other rule.

To add a custom network adapter to the network adapter list

1. In the console, click **Policies > Policy Components > Network Adapters**.
2. Under **Tasks**, click **Add a Network Adapter**.
3. In the **Network Adapter** dialog box, in the **Adapter Type** drop-down list, select an adapter.
4. In the **Adapter Name** field, optionally type a description.
5. In the **Adapter Identification** text box, type the case-sensitive brand name of the adapter.

To find the brand name of the adapter, open a command line on the client, and then type the following text:

```
ipconfig/all
```

6. Click **OK**.

More information

- [Managing firewall rules](#)
- [About firewall rule network adapter triggers](#)
- [Controlling the traffic that passes through a network adapter](#)

Copying Symantec Endpoint Protection firewall rules

Quickly create SEP Firewall rules. Exporting a Firewall rule from a policy and then importing the rule into a different policy. You can also save time creating rules by exporting an existing Firewall rule that contains settings that you want to reuse. Then import the rule into a policy and modify it.

Rules are exported to a .dat file. Ensure that you have access to the .dat file when you are ready to import the rule. Rules are added in the same order that they appear in the parent policy with respect to the blue line. After you import the rule, you can change the processing order.

To export firewall rules

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.
For versions earlier than 14.2, there is no option for **Mac Settings**.
3. In the **Rules** list, select the rules that you want to export, right-click, and then click **Export**.
4. In the **Export Policy** dialog box, locate a directory to save the .dat file, type a file name, and then click **Export**.

To import firewall rules

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.
For versions earlier than 14.2, there is no option for **Mac Settings**.

-
3. Right-click the Rules list, and then click **Import**.
 4. In the **Import Policy** dialog box, locate the .dat file that contains the firewall rules to import, and then click **Import**.
 5. In the **Input** dialog box, type a new name for the policy, and then click **OK**.
 6. Click **OK**.

More information

- [Adding a new firewall rule](#)
- [Customizing firewall rules](#)
- [About the firewall rule, firewall setting, and intrusion prevention processing order](#)

Customizing firewall rules

When you create a new Firewall policy, the policy includes several default rules. You can modify one or multiple rule components as needed.

Table 76: Components of a firewall rule

Actions	The action parameters specify what actions the firewall takes when it successfully matches a rule. If the rule matches and is selected in response to a received packet, the firewall performs all actions. The firewall either allows or blocks the packet and logs or does not log the packet. If the firewall allows traffic, it lets the traffic that the rule specifies access the network. If the firewall blocks traffic, it blocks the traffic that the rule specifies so that it does not access the network. The actions are as follows: • Allow The firewall allows the network connection. • Block The firewall blocks the network connection. Note: The Mac client firewall monitors packets but does not log them. Note: This note applies only as of 14.2.
Triggers	When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any one trigger is not true in relation to the current packet, the firewall cannot apply the rule. You can combine the trigger definitions to form more complex rules, such as to identify a particular protocol in relation to a specific destination address. The triggers are as follows: • Application When the application is the only trigger you define in an allow-traffic rule, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed. See: About firewall rule application triggers • Host When you define host triggers, you specify the host on both sides of the described network connection. Traditionally, the way to express the relationship between hosts is referred to as being either the source or destination of a network connection. See: About firewall rule host triggers • Network services A network services trigger identifies one or more network protocols that are significant in relation to the described traffic. The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic. See: About firewall rule network services triggers • Network adapter If you define a network adapter trigger, the rule is relevant only to the traffic that is transmitted or received by using the specified type of adapter. You can specify either any adapter or the one that is currently associated with the client computer. See: About firewall rule network adapter triggers
Conditions	Rule conditions consist of the rule schedule and screen saver state. The conditional parameters do not describe an aspect of a network connection. Instead, the conditional parameters determine the active state of a rule. You may define a schedule or identify a screen saver state that dictates when a rule is considered to be active or inactive. The conditional parameters are optional and if not defined, not significant. The firewall does not evaluate inactive rules.
Notifications	The Log settings let you specify whether the server creates a log entry or sends an email message when a traffic event matches the criteria that are set for this rule. The Severity setting lets you specify the severity level of the rule violation.

To customize firewall rules

-
1. In the console, open a Firewall policy.
 2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.
For versions earlier than 14.2, there is no option for **Mac Settings**.
 3. On the **Rules** tab, in the **Rules** list, in the **Enabled** field, ensure that the box is checked to enable the rule; uncheck the box to disable the rule.
Symantec Endpoint Protection only processes the rules that you enable. All rules are enabled by default.
 4. Double-click the **Name** field and type a unique name for the firewall rule.
 5. Right-click the **Action** field and select the action that you want Symantec Endpoint Protection to take if the rule is triggered.
 6. In the **Application** field, define an application. See:
[Defining information about applications](#)
 7. In the **Host** field, specify a host trigger. See:
[Blocking traffic to or from a specific server](#)
 8. In addition to specifying a host trigger, you can also specify the traffic that is allowed to access your local subnet. See:
[Allowing only specific traffic to the local subnet](#)
 9. In the **Service** field, specify a network service trigger. See:
[Controlling whether networked computers can share messages, files, and printing](#)
 10. In the **Log** field, specify when you want Symantec Endpoint Protection to send an email message to you when this firewall rule is violated. See:
[Setting up notifications for firewall rule violations](#)
 11. Right-click the **Severity** field and select the severity level for the rule violation.
 12. In the **Adapter** column, specify an adapter trigger for the rule. See:
[Controlling the traffic that passes through a network adapter](#)
 13. In the **Time** column, specify the time periods in which this rule is active.
 14. Right-click the **Screen Saver** field and specify the state that the client computer's screen saver must be in for the rule to be active.
The **Created At** field is not editable. If the policy is shared, the term Shared appears. If the policy is not shared, the field shows the name of the group to which that the non-shared policy is assigned.
 15. Right-click the **Description** field, click **Edit**, type an optional description for the rule, and then click **OK**.
 16. If you are done with the configuration of the rule, click **OK**.

More information

- [Adding a new firewall rule](#)
- [Managing firewall rules](#)

Blocking traffic to or from a specific server

To block traffic to or from a specific server, you can block the traffic by IP address rather than by domain name or host name. Otherwise, the user may be able to access the IP address equivalent of the host name.

To block traffic to or from a specific server

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Host** field, and then click **Edit**.
4. In the **Host List** dialog box, do one of the following actions:
 - Click **Source/Destination**.
 - Click **Local/Remote**.
5. Do one of the following tasks:

To select a host type from the Type drop-down list	Do all of the following tasks: • In the Source and Destination or Local and Remote tables, click Add. • In the Host dialog box, select a host type from the Type drop-down list, and type the appropriate information for each host type. • Click OK. The host that you created is automatically enabled.
To select a host group	In the Host List dialog box, do one of the following actions: • Click Source/Destination. • Click Local/Remote. Then in the Host List dialog box, check the box in the Enabled column for any host group that you want to add to the rule.

6. Add additional hosts, if necessary.
7. Click **OK** to return to the **Rules** list.

More information

- [Adding a new firewall rule](#)
- [Customizing firewall rules](#)
- [Adding host groups](#)

Allowing only specific traffic to the local subnet

You can create a firewall rule that permits only specific traffic to your local subnet. This firewall rule always applies to your local subnet IP address, regardless of what the address is. Therefore, even if you change your local subnet IP address, you never have to modify this rule for the new address.

For example, you can create this rule to permit traffic to port 80 only on the local subnet, regardless of what the local subnet IP address is.

To allow only specific traffic to the local subnet

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.

For versions earlier than 14.2, there is no option for **Mac Settings**.

-
3. On the **Rules** tab, in the **Firewall Rules** table, find the rule that you want to edit.
 4. Double-click in the **Host** column for the rule for which you want to create a local subnet traffic condition.
 5. Under the type of hosts for which this rule applies (Local or Remote), click **Add**.
 6. Click the **Address Type** drop-down list and select one of the following:
 - Windows: **Local Subnet**
 - Mac: **Subnet**
 7. Click **OK**, and then click **OK** again to close out of the **Host List** dialog box.

More information

[Customizing firewall rules](#)

Controlling whether networked computers can share messages, files, and printing

Network services let networked computers send and receive messages, shared files, and print. You can create a firewall rule that allows or blocks network services.

You can add a custom network service through a firewall rule. However, that network service is not added to the default list. You cannot access the custom service from any other rule.

To control whether networked computers can share messages, files, and printing

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.

For versions earlier than 14.2, there is no option for **Mac Settings**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
4. In the **Service List** dialog box, check the box beside each service that you want to trigger the rule.
5. To add an additional service for the selected rule only, click **Add**.
6. In the **Protocol** dialog box, select a protocol from the **Protocol** drop-down list.
7. Fill out the appropriate fields.
8. Click **OK**.
9. Click **OK**.
10. Click **OK**.

More information

- [Adding a new firewall rule](#)
- [Customizing firewall rules](#)
- [About firewall rule network services triggers](#)
- [Adding network services to the default network services list](#)

Permitting clients to browse for files and printers in the network

You can enable the client to either share its files or to browse for shared files and printers on the local network. To prevent network-based attacks, you may not want to enable network file and printer sharing.

You enable network file and print sharing by adding firewall rules. The firewall rules allow access to the ports to browse and share files and printers. You create one firewall rule so that the client can share its files. You create a second firewall rule so that the client can browse for other files and printers.

The settings work differently based on the type of control that you specify for your client, as follows:

Client control or mixed control	Users on the Windows client can enable these settings automatically by configuring them in Network and Host Exploit Mitigation. Users on the Mac client can only enable or disable the firewall.
Mixed control	A server firewall rule that specifies this type of traffic can override these settings on Windows. All firewall rules are server firewall rules on a Mac.
Server control	These settings are not available on the client.

To permit Windows clients to browse for files and printers in the network (Option 1)

1. On the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings**, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
4. In the **Service List** dialog box, click **Add**.
5. In the **Protocol** dialog box, in the **Protocol** drop-down list, click **TCP**, and then click **Local/Remote**.
6. Do one of the following tasks:

To permit clients to browse for files and printers in the network	In the Remote port drop-down list, type 88, 135, 139, 445.
To enable other computers to browse files on the client	In the Local Port drop-down list, type 88, 135, 139, 445.

7. Click **OK**.
8. In the **Service List** dialog box, click **Add**.
9. In the **Protocol** dialog box, in the **Protocol** drop-down list, click **UDP**.
10. Do one of the following tasks:

To permit clients to browse for files and printers in the network	In the Local Port drop-down list, type 137, 138. In the Remote Port drop-down list, type 88.
To enable other computers to browse files on the client	In the Local Port drop-down list, type 88, 137, 138.

11. Click **OK**.
12. In the **Service List** dialog box, make sure that the two services are enabled, and then click **OK**.
13. On the **Rules** tab, make sure the **Action** field is set to **Allow**.
14. If you are done with the configuration of the policy, click **OK**.

To permit Mac clients to browse for files and printers in the network (Option 2)

1. In the console, open a Firewall policy.

NOTE

The Mac firewall is available as of version 14.2.

2. On the **Firewall Policy** page, under **Mac Settings**, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Service** field, and then click **Edit**.
4. In the **Service List** dialog box, click **Add**.
5. In the **Protocol** dialog box, in the **Protocol** drop-down list, click **TCP**, and then click **Local/Remote**.
6. To enable other computers to browse files on the client, in the **Local Port** drop-down list, type 139 and 445.
Outgoing requests to browse the network from the Mac are enabled by default.
7. Click **OK**.

-
8. In the **Service List** dialog box, make sure that the new service is enabled, and then click **OK**.
 9. On the **Rules** tab, make sure the **Action** field is set to **Allow**.
 10. If you are done with the configuration of the policy, click **OK**.

Printer discovery on Macs is through the Bonjour service, which is open by default. You do not need to configure a custom rule for the Bonjour service.

Printer discovery on Macs is through the Bonjour service, which is open by default. You do not need to configure a custom rule for the Bonjour service.

More information

- [Adding a new firewall rule](#)
- [Customizing firewall rules](#)

Setting up notifications for firewall rule violations

You can configure Symantec Endpoint Protection to send you an email message each time the firewall detects a rule violation, attack, or event. For example, you may want to know when a client blocks the traffic that comes from a particular IP address.

To set up notifications for firewall rule violations

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Rules**.
For versions earlier than 14.2, there is no option for **Mac Settings**.
3. On the **Rules** tab, select a rule, right-click the **Log** field, and do one or more of the following tasks:

To send an email message when a firewall rule is triggered	Check Send Email Alert .
To generate a log event when a firewall rule is triggered	For Windows rules, check both Write to Traffic Log and Write to Packet Log . For Mac rules, check Write to Traffic Log .

4. When you are done with the configuration of this policy, click **OK**.
5. Configure a security alert.
6. Configure a mail server.
7. Click **OK**.

More information

- [Adding a new firewall rule](#)
- [Customizing firewall rules](#)
- [Setting up administrator notifications](#)

Controlling the traffic that passes through a network adapter

When you define a network adapter trigger, the rule is relevant only to the traffic that the specified adapter transmits or receives.

You can add a custom network adapter from a firewall rule. However, that adapter is not added to the shared list. You cannot access the custom adapter from any other rule.

To control the traffic that passes through a network adapter

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings**, click **Rules**.
3. On the **Rules** tab, in the **Rules** list, select the rule you want to edit, right-click the **Adapter** field, and then click **More Adapters**.
4. In the **Network Adapter** dialog box, do one of the following actions:

To trigger the rule for any adapter (even if it is not listed)	Click Apply the rule to all adapters , and then go to step 7.
To trigger the rule for selected adapters	Click Apply the rule to the following adapters . Then check the box beside each adapter that you want to trigger the rule.

5. To add a custom adapter for the selected rule only, do the following tasks:
 - Click **Add**.
 - In the **Network Adapter** dialog box, select the adapter type and type the adapter's brand name in the **Adapter Identification** text field.
6. Click **OK**.
7. Click **OK**.
8. Click **OK**.

More information

- [Adding a new firewall rule](#)
- [Customizing firewall rules](#)
- [About firewall rule network adapter triggers](#)

Configuring firewall settings for mixed control

You can configure the client so that users have no control, full control, or limited control over which firewall settings they can configure.

For the Mac firewall, the user cannot create firewall rules or change settings regardless of the client user interface settings. The options do not ever appear in the client user interface.

Server control	For Windows, the user cannot create any firewall rules or enable firewall settings. For Mac, the user cannot enable or disable the firewall.
Client control	For Windows, the user can create firewall rules and enable all firewall settings. For Mac, the user can enable and disable the firewall.
Mixed control	For Windows, the user can create firewall rules. You decide which firewall settings the user can enable. For Mac, you decide whether the user can enable or disable the firewall.

NOTE

The firewall is only available for the Mac client as of version 14.2.

To configure firewall settings for mixed control

-
1. In the console, click **Clients**.
 2. Under **Clients**, select the group with the user control level that you want to modify.
 3. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
 4. To the right of **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
 5. In the **Control Mode Settings** dialog box, click **Mixed control**, and then click **Customize**.
 6. On the **Client/Server Control Settings** tab, under the **Firewall Policy** category, do one of the following tasks:
 - To make a client setting available for the users to configure, click **Client**.
 - To configure a client setting, click **Server**.
 7. Click **OK**.
 8. Click **OK**.
 9. For each firewall setting that you set to **Server**, enable or disable the setting in the Firewall policy.

More information

- [Managing firewall protection](#)
- [Enabling communications for network services instead of adding a rule](#)

Enabling communications for network services instead of adding a rule

You can enable the options that automatically allow communication between certain network services so you do not have to define the rules that explicitly allow those services. You can also enable traffic settings to detect and block the traffic that communicates through NetBIOS and token rings.

You can allow outbound requests and inbound replies for the network connections that are configured to use DHCP, DNS, and WINS traffic.

The filters allow DHCP, DNS, or WINS clients to receive an IP address from a server. It also protects the clients against attacks from the network with the following conditions:

If the client sends a request to the server	The client waits for five seconds to allow an inbound response.
If the client does not send a request to the server	Each filter does not allow the packet.

When you enable these options, Symantec Endpoint Protection permits the packet if a request was made; it does not block packets. You must create a firewall rule to block packets.

NOTE

To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To enable communications for network services instead of adding a rule

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page, under **Windows Settings** or **Mac Settings**, click **Built-in Rules**.

For versions earlier than 14.2, these settings are for Windows only.

-
3. Check the options that you want to enable.
 4. Click **OK**.
 5. If you are prompted, assign the policy to a location.

More information

- [Creating a firewall policy](#)
- [Editing a policy](#)
- [Preventing users from disabling protection on client computers](#)

Automatically blocking connections to an attacking computer

If the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an Active Response, which automatically blocks all communication to and from the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.

The attacker's IP address is recorded in the Security log. You can unblock an attack by canceling a specific IP address or canceling all Active Response.

If you set the client to mixed control, you can specify whether the setting is available on the client for the user to enable. If it is not available, you must enable it in the **Client User Interface Mixed Control Settings** dialog box.

Updated IPS signatures, updated denial-of-service signatures, port scans, and MAC spoofing also trigger an Active Response.

To automatically block connections to an attacking computer

1. In the console, open a Firewall policy.
2. On the **Firewall Policy** page in the left pane, click one of the following options:
 - Under **Windows Settings: Protection and Stealth**
 - Under **Mac Settings: Protection**
Mac settings are available only as of version 14.2.
3. Under **Protection Settings**, check **Automatically block an attacker's IP address**.
4. In the **Number of seconds during which to block IP address ... seconds** text box, specify the number of seconds to block potential attackers.
You can enter a value from 1 to 999,999.
5. Click **OK**.

More information

- [Creating a firewall policy](#)
- [Configuring firewall settings for mixed control](#)
- [Editing a policy](#)

Detecting potential attacks and spoofing attempts

You can enable the various settings that enable Symantec Endpoint Protection to detect and log potential attacks on the client and block spoofing attempts. All of these options are disabled by default.

Table 77: Settings that you can enable

Setting	Description
Enable port scan detection	When this setting is enabled, Symantec Endpoint Protection monitors all incoming packets that any security rule blocks. If a rule blocks several different packets on different ports in a short period of time, Symantec Endpoint Protection creates a Security log entry. Port scan detection does not block any packets. You must create a security policy to block traffic when a port scan occurs.
Enable denial of service detection	Denial of service detection is a type of intrusion detection. When enabled, the client blocks traffic if it detects a pattern from known signatures, regardless of the port number or type of Internet protocol.
Enable anti-MAC spoofing	When this setting is enabled, Symantec Endpoint Protection allows the following incoming and outgoing traffic if a request was made to that specific host: • Address resolution protocol (ARP) (IPv4) • Neighbor Discovery Protocol (NDP) (IPv6) Supported as of version 14.2. All other unexpected traffic is blocked and an entry is generated to the Security log.

NOTE

To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

To detect potential attacks and spoofing attempts

1. In the console, open a Firewall policy.
2. In the **Firewall Policy** page, click one of the following:
 - Under **Windows Settings: Protection and Stealth**
 - Under **Mac Settings: Protection**Mac settings are available only as of version 14.2.
3. Under **Protection Settings**, check any of the options that you want to enable.
4. Click **OK**.
5. If you are prompted, assign the policy to a location.

More information

- [Creating a firewall policy](#)
- [Preventing users from disabling protection on client computers](#)
- [Editing a policy](#)

Preventing outside stealth attacks on computers

You can enable the settings that prevent outside attacks from detecting information about your clients. These settings are disabled by default.

NOTE

To configure these settings in mixed control, you must also enable these settings in the **Client User Interface Mixed Control Settings** dialog box.

NOTE

These stealth settings are not available for the Mac firewall.

To prevent outside stealth attacks on computers

1. In the console, open a Firewall policy.
2. In the **Firewall Policy** page, click **Protection and Stealth**.
3. Under **Stealth Settings**, check any of the options that you want to enable.
4. Click **OK**.
5. If you are prompted, assign the policy to a location.

More information

- [Creating a firewall policy](#)
- [Preventing users from disabling protection on client computers](#)
- [Editing a policy](#)

About firewall settings for the Mac client

The firewall settings that are included in the Symantec Endpoint Protection client for Mac are as follows:

- Firewall smart rules
- Custom firewall rules

These settings are only configurable by the Symantec Endpoint Protection Manager administrator. The firewall is only available to managed clients.

The firewall is included with the Symantec Endpoint Protection client for Mac as of version 14.2.

Table 78: Firewall settings

Setting type	Description
Firewall smart rules	Firewall smart rules provide protection to prevent common types of attack. They also allow traffic on specific protocols when the Mac makes the initial request on that protocol. Protection settings include: • Portscan detection • Denial of service detection • Anti-MAC spoofing • Automatically block an attacker's IP address Traffic protocols include: • Smart DHCP • Smart DNS The Symantec Endpoint Protection firewall for Mac does not integrate with the operating system's built-in firewall. Instead, it runs in parallel. The operating system firewall inspects at the Application layer, while the Symantec Endpoint Protection firewall inspects at lower levels (Network and Transport). The Symantec Endpoint Protection firewall for Mac does not offer peer-to-peer blocking rules, though you could create these in part through custom firewall rules.
Custom firewall rules	Custom firewall rules allow the administrator to create the rules that involve various attributes of the network traffic.

More information

[Managing firewall protection](#)

Disabling the Windows Firewall

You can specify the conditions in which Symantec Endpoint Protection disables Windows Firewall. Symantec Endpoint Protection restores the Windows Firewall settings to the state it was in before Symantec Endpoint Protection was installed when the following occurs:

- Symantec Endpoint Protection is uninstalled.
- The Symantec Endpoint Protection firewall is disabled.

NOTE

Symantec Endpoint Protection does not modify any existing Windows Firewall policy rules or exclusions.

Typically, a Windows user receives a notification when their computer restarts if Windows Firewall is disabled. Symantec Endpoint Protection disables this notification by default so that it does not alarm your users when Windows Firewall is disabled. However, you can enable the notification, if desired.

To disable the Windows Firewall

1. In the console, click **Policies**.
2. Under **Policies**, click **Firewall**.
3. Do one of the following tasks:
 - Create a new firewall policy.
 - In the **Firewall Policies** list, double-click on the firewall policy that you want to modify.
4. Under **Firewall Policy**, click **Windows Integration**.
5. In the **Disable Windows Firewall** drop-down list, specify when you want Windows Firewall disabled.

The default setting is **Disable Once Only**.

Click **Help** for more information on the options. See:

[Windows Integration](#)

6. In the **Windows Firewall Disabled Message** drop-down list, specify whether you want to disable the Windows message on startup to indicate that the firewall is disabled.

The default setting is **Disable**, which means the user does not receive a message upon a computer startup that Windows Firewall is disabled.

7. Click **OK**.

More information

- [Creating a firewall policy](#)
- [The types of security policies](#)

Configuring intrusion prevention

Protect your endpoints against ransomware and malware with the Intrusion Prevention System (IPS). IPS is the first layer of defense against malware after the firewall on Windows and Mac clients.

What is intrusion prevention and what does it do?

Intrusion Prevention:

- Blocks over 70% of attacks before they break into your organization's network. Even after malware breaks into your organization, IPS detects malware in the infestation and exfiltration phase. During this phase, IPS blocks threats as they travel through the network.
- Detects ransomware attacks by using the URL reputation, which prevents web threats.
- Is a one-of-a-kind protection that no other security company uses.

IPS blocks malware at the network layer before the payload arrives on the endpoint, as it scans both inbound and outbound network traffic. IPS is able to:

- Recognize and understand various network protocols and provide custom protection for each type.
- Use pattern matching to identify unknown and known threats.
- Block command-and-control (C&C) communications to known malicious URLs and IP addresses using Symantec's Insight Intelligence.

On Endpoint Security, IPS uses over 400 of audit signatures. Audit signatures are signatures that do not have a default action.

NOTE

Symantec recommends that you install the client software on servers as well as desktop computers. In addition, Symantec recommends that you move server endpoints to the same group.

For more information about signatures, see:

[About Symantec IPS signatures](#)

Step 1: Enable intrusion prevention

IPS is enabled by default so that your computers are always protected.

NOTE

Symantec recommends that you always keep IPS enabled.

The following IPS capabilities are also enabled by default:

Capability	Description
Browser protection (Browser Intrusion Prevention for Windows)	IPS web browser signatures allow and block inbound and outbound browser traffic. The Google Chrome browser extension (14.3 RU2 and later) and Microsoft InTune extension (14.3 RU8 and later) are installed by default. Integrating browser extensions with Symantec Endpoint Protection (SEP) to protect against malicious websites
Network Intrusion Prevention	Network IPS signatures protect against network attacks.
URL reputation	URL reputation detections identify threats from domains and URLs, which can host malicious content like malware, fraud, phishing, and spam, etc. URL reputation blocks access to web addresses that are identified as known sources of malicious content. The information from visited URLs is sent to Symantec to retrieve a reputation rating. A URL is believed to be incorrectly detected by the Endpoint Security/Endpoint Protection URL Reputation feature resulting in a False Positive. Note: If the client incorrectly detected a URL as hosting malicious content, submit the URL as a false positive. See: Note: URL Reputation False Positive Process

For servers that have the client software installed on them, enable the following settings in the **Intrusion Prevention** policy:

Out-of-band scanning	Applies multi-threaded scans to improve performance.
Use signature subset for servers	Applies signatures that prevent the most commonly known threats on servers.

Endpoint Protection performance tuning settings:

Server Performance Tuning

Server performance tuning helps to improve the performance of intrusion prevention on server operating systems.

☐ Out-of-band scanning

Note: This option may have compatibility issues with other Windows Filtering Platform (WFP) drivers. Therefore, if you enable this option, apply the policy to a test server to test it before you apply it to all production servers.

☐ Use signature subset for servers

Endpoint Security performance tuning settings:

Server Performance Tuning [Hide Advanced](#)

Use signature subset for servers



Out-of-band scanning



For more information about tuning settings, see:

- [Enabling intrusion prevention](#)
- [URL Reputation FAQ](#)
- [Integrating browser extensions with Symantec Endpoint Protection \(SEP\) to protect against malicious websites](#)

Step 2: Block ransomware by using URL reputation (14.3 RU2 and later)

IPS is the best defense against drive-by downloads, which occur when software is unintentionally downloaded from the Internet. Attackers often use exploit kits to deliver a web-based attack like CryptoLocker through a drive-by download.

In some cases, IPS can block file encryption by interrupting command-and-control (C&C) communication. A C&C server is a computer that an attacker or cybercriminal controls to send commands to systems compromised by malware in order to receive stolen data from a target network.

For 14.3 RU2 and later clients, URL reputation blocks these drive-by downloads, as long as URL reputation is enabled.

Endpoint Protection URL reputation settings:

Prevention Policy

tion

ettings

gs

Intrusion Prevention

Intrusion Prevention
Network Intrusion Prevention automatically detects and blocks network intrusions and blocks browser attacks.

 ☒ Enable Network Intrusion Prevention

☒ Enable excluded hosts

 ☒ Enable Browser Intrusion Prevention for Windows

☐ Log detections but do not block

 ☒ Enable URL reputation

Endpoint Security URL reputation settings:

Advanced Settings 

Intrusion Prevention

Browser Protection [Show Advanced](#)

Enable URL reputation

Server Performance Tuning [Show Advanced](#)

 [Also supports](#) 





For more information about URL reputation settings, see:

[Ransomware protection using Symantec Endpoint Protection](#)

Step 3: (Optional) Add custom IPS signatures

To identify a specific intrusion and reduce the possibility of signatures that cause a false positive, you can write your own custom network intrusion prevention signatures. The more information that you can add to a custom signature, the more effective the signature is.

NOTE

Custom IPS signatures are only available in Symantec Endpoint Protection. They will be available in Symantec Endpoint Security soon.

Intrusion Prevention Policies Custom Intrusion Prevention Signatures

Name	Description	Group and Location Use Count
------	-------------	------------------------------

Custom Intrusion Prevention Signatures

×

Name:

New Custom Intrusion Prevention Signatures

Description:

You can follow this sample to create your own custom Intrusion Prevention signatures.

Signatures

Variables

Signature Groups

NetBIOS Group

Group Name:

NetBIOS Group

Description:

This is an example of a NetBIOS signature group.

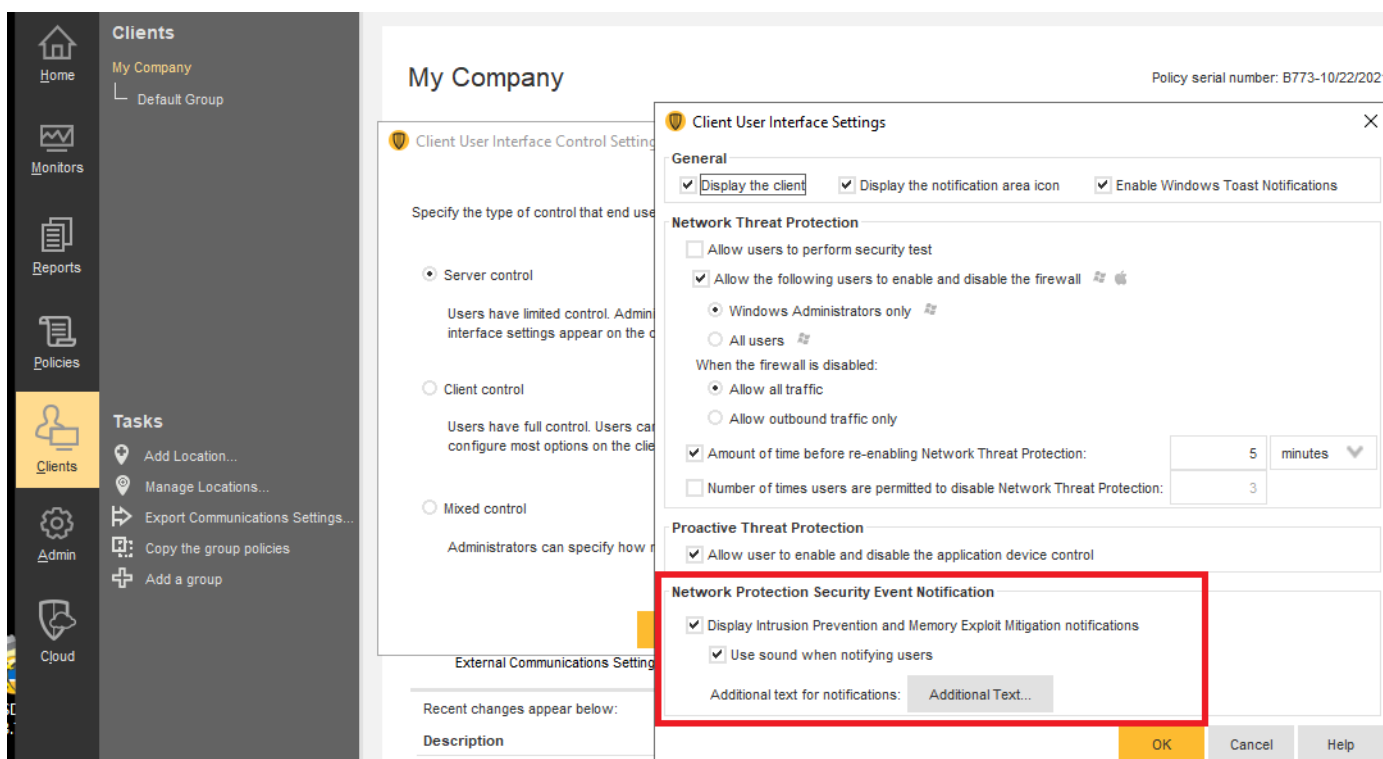
☒ Enable this group

Signatures for this Group

Enabled	Name	Content	Applications	Action	Track
☒	NetBIOS DoS R...	rule tcp, dest=(...	*	Block	Log

- Managing custom intrusion prevention signatures
- About custom IPS signatures

When IPS detects suspicious activity on the client, it sends a notification to client users. You can keep the default notification text or replace it with a custom message.



For more information about notification settings, see:

[Configuring client notifications for intrusion prevention and Memory Exploit Mitigation](#)

Endpoint Security notification settings:

User Notification Settings ?

Notifications are only sent for enabled signatures.

Show notification on the device

[Hide Advanced](#)

Show a custom notification on the device

Step 5: (Optional) Run a report on IPS detections

To gain better visibility into IPS detections and the network security posture of your organization, run the following reports:

- In Symantec Endpoint Protection, run a **Network and Host Exploit Mitigation** report.
- In Symantec Endpoint Security, run an **Intrusion Prevention** report.

Endpoint Protection report settings:

[Home](#)[Monitors](#)[Reports](#)[Policies](#)[Clients](#)[Admin](#)[Cloud](#)[Quick Reports](#)[Scheduled Reports](#)

Network and Host Exploit Mitigation Reports

What type of report would you like to see?

Report type: Network and Host Exploit Mitigation

Select a report: Full Report

Use a saved filter: Default

What filter settings would you like to use?

Time range: Past 24 hours

[Additional Settings >>](#)

Reports to Include

Reports to Include

Specify the reports you want to include:

- ☒ Top Types of Attack
- ☒ Top Targets Attacked by Group
- ☒ Top Targets Attacked by Subnet
- ☒ Top Targets Attacked by Client
- ☒ Top Sources of Attack
- ☒ Top Traffic Notifications by Group (Traffic)
- ☒ Top Traffic Notifications by Group (Packets)
- ☒ Top Traffic Notifications by Subnet (Traffic)
- ☒ Top Traffic Notifications by IPv6 Subnet (Traffic)
- ☒ Top Traffic Notifications by Subnet (Packets)
- ☒ Top Traffic Notifications by IPv6 Subnet (Packets)

For more information about reports, see:

[Running and customizing quick reports](#)

Endpoint Security report settings:

The IPS signatures detect threats that may or may not be malware. If you think that the signature is not associated with potentially malicious activity in your environment and is a false positive, you can create an exception to prevent IPS from using that signature.

1. Add exceptions.

To add exceptions

- For more information, see:

2. Create custom IPS signatures.

NOTE

3. **Exclude specific computers based on their IP addresses so that the IPS engine does not scan them.**

For example, you might exclude computers to allow an Internet service provider to scan the ports in your network to ensure compliance with their service agreements. Or, you might have some computers in your internal network that you want to set up for testing.

Endpoint Protection excluded hosts settings:

Intrusion Prevention

Intrusion Prevention

Network Intrusion Prevention automatically detects and blocks network attacks. It also blocks browser attacks.



☒ Enable Network Intrusion Prevention



Enable excluded hosts

Excluded Hosts...



Excluded Hosts

Host List

Hosts to exclude from Intrusion Prevention:

Enabled	Group Name
---------	------------

For more information about excluded host settings, see:

[Setting up a list of excluded computers](#)

Endpoint Security host exclusion settings (in the Allow List):

Intrusion Prevention Host Exclusion ⓘ

List of excluded hosts

[+ Add](#)

HOST TYPE	HOST SPECIFICATION
-----------	--------------------

No IPS hosts added.

For more information about host exclusion settings, see:

[Adding Allow List policy scan exceptions](#)

4. **If you think that URL reputation triggers a known good URL, submit the URL to the Symantec security team.**

Follow the steps in the following Support article:

[URL Reputation False Positive Process](#)

Endpoint Protection exceptions settings:

Intrusion Prevention Policy

Overview

Intrusion Prevention

Windows Settings

Exceptions

Mac Settings

Exceptions

Exceptions

Intrusion
Select s

ID

Add Intrusion Prevention Exceptions

Intrusion Prevention Exceptions

Select the signatures that need settings that are different from the default settings.

Show category:

All

Show severity

ID	Signature Name	Severity	Categories
20632	System Infected: BD BackOrifice 2000 UD...	High	Intrusion Preven
20119	System Infected: BD NetBus Activity	High	Intrusion Preven
20042	Attack: DDOS Mstream HandlerAgent Com...	High	Server Signature
20068	OS Attack: SMB Request Buffer Overflow ...	Medium	Server Signature

Endpoint Security exceptions settings:

Signature Action Exceptions

Also supports

Search Signatures



Showing list of Signatures



Enable



Log



Disable



Remove



Add



SIGNA...

PLATF...

SIGNATURE NAME

SEVER...

CATEGORY

STATUS

How intrusion prevention works

Intrusion prevention automatically detects and blocks network attacks. On Windows computers, intrusion prevention also detects and blocks browser attacks on supported browsers. Intrusion prevention is the second layer of defense after the firewall to protect client computers. Intrusion prevention is sometimes called the intrusion prevention system (IPS).

Intrusion prevention intercepts data at the network layer. It uses signatures to scan packets or streams of packets. It scans each packet individually by looking for the patterns that correspond to network attacks or browser attacks. Intrusion prevention detects attacks on operating system components and the application layer.

The following IPS capabilities are also enabled by default:

Table 79: IPS functionality

Type	Description
Network intrusion prevention	Network intrusion prevention uses signatures to identify attacks on client computers. For known attacks, intrusion prevention automatically discards the packets that match the signatures.
Browser protection (Windows only)	Browser protection (or <i>browser intrusion prevention</i>) monitors attacks on browsers, including Internet Explorer, Firefox, and Chrome. Firefox might disable the Symantec Endpoint Protection plug-in, but you can turn it back on. Intrusion prevention uses attack signatures as well as heuristics to identify attacks on browsers. For some browser attacks, intrusion prevention requires that the client terminate the browser. A notification appears on the client computer. For the latest information about the browsers that browser intrusion prevention protects, see: Supported browser versions for browser intrusion prevention

Type	Description
URL reputation	URL reputation detections identify threats from domains and URLs, which can host malicious content like malware, fraud, phishing, and spam, etc. URL reputation blocks access to the web addresses that are identified as known sources of the malicious content. The information from visited URLs is sent to Broadcom to retrieve a reputation rating.

See: [Configuring intrusion prevention](#)

Enabling intrusion prevention

Intrusion prevention is enabled by default. Typically, you should not disable intrusion prevention except to troubleshoot.

You can enable a log-only mode for browser intrusion prevention to record what traffic it blocks without affecting the client user. You can then use the **Network and Host Exploit Mitigation** attack logs in Symantec Endpoint Protection Manager to create exceptions in the **Intrusion Prevention** policy to ignore specific browser signatures. You would then disable log-only mode.

NOTE

To make these settings available for the client user to enable or disable, configure these settings in the **Client User Interface Mixed Control Settings** dialog box.

To enable intrusion prevention

1. In the console, open an Intrusion Prevention policy.
2. On the policy page, click **Intrusion Prevention**.
3. Make sure the following options are checked:
 - **Enable Network Intrusion Prevention**
You can also exclude particular computers from network intrusion prevention. See: [Setting up a list of excluded computers](#)
 - **Enable Browser Intrusion Prevention for Windows**
Unchecking this option also lets you uninstall the Google Chrome browser extension (14.3 RU5 or later) and the Microsoft Edge Browser extension (14.3 RU8 or later).
4. Click **OK**.

More information

- [Creating exceptions for IPS signatures](#)
- [Managing intrusion prevention](#)
- [Configuring firewall settings for mixed control](#)

Integrating browser extensions with Symantec Endpoint Protection (SEP) to protect against malicious websites

What is the SEP browser extension?

Browser extensions are plug-ins that add functionality and features to a web browser. The SEP browser extension monitors inbound and outbound HTTP and HTTPS traffic to the web browser and blocks the traffic if the client determines that the URL is malicious. If the web browser detects that a URL is malicious, the client then redirects users to a [default landing page](#).

Symantec Endpoint Protection offers Browser Protection for the following browsers:

-
- Version 14.3 RU8 and later installs a Microsoft Edge extension.
 - Version 14.3 RU2 and later installs a Google Chrome extension.
 - Mozilla Firefox and Microsoft Internet Explorer do not use a browser extension. Instead, SEP supports these browsers based on the version of the Client Intrusion Detection System (CIDS) engine that the client uses.

How does the SEP browser extension work?

The SEP browser extension identifies and protects malicious URLs using the following techniques:

- Browser intrusion prevention (also called Browser Protection) applies the IPS web browser signatures to the inbound and the outbound browser traffic on the Windows client. See:
[Expected behavior of Browser Intrusion Prevention](#)
- **URL reputation** identifies threats from domains and URLs that can host malicious content like malware, fraud, phishing, and spam. URL reputation then blocks access to the web addresses that are identified as known sources of the malicious content. See:
[SEP URL Reputation FAQ](#)

After the Chrome or Edge browser extension is installed, LiveUpdate downloads a sub-feature of IPS, called WebExt. The browser extension uses WebExt definitions and IPS signatures.

WebExt definitions include the following components:

- **WebFilter:** Uses the extension engine WebPulse to inspect the URLs based on the domain and category. WebPulse uses Insight and reputation lookup.
- **Scanner:** A scan file that uses IPS signatures to report detections.

One difference between the kernel IPS is that the IPS cannot see HTTPS traffic, whereas the browser extension can.

Step 1: Before you install the SEP browser extension

Before you install the SEP browser extension, complete the following tasks:

1. Make sure that the client installation package includes both the **Advanced Download Protection** and the **Intrusion Prevention** components. The browser extension depends on IPS. See:
[Choosing which security features to install on the client](#)
2. Make sure that the Live Update Browser Extension content is enabled.
LiveUpdate automatically installs these definitions by default. You enable this content by clicking **Admin > Servers > Edit Site Properties > LiveUpdate tab > Content Types to Download > Browser Extension**. See:
[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)
3. Choose whether you want to install the SEP browser extension from Symantec Endpoint Protection Manager directly or you want to use a third-party management console.
See: [Step 2: Choose a method to install the SEP browser extension](#)
4. (Optional) To minimize false positives, create an exception to allow web domains so that the client never blocks them. In the Exceptions policy, add a Windows **Trusted Web Domain** exception. See:
[Trusted Web Domain Exception](#)

Step 2: Choose a method to install the SEP browser extension

The following table describes the ways that you can install the SEP browser extension on Google Chrome or Microsoft Edge.

NOTE

When you configure policies using the following methods, `HKEY_LOCAL_MACHINE` takes precedence over the cloud user policy, which takes precedence over `HKEY_CURRENT_USER`.

Table 80: Methods for installing the SEP Browser Extension

Method	When to use	How to configure
The Symantec Endpoint Protection client installer (default)	You want to install the SEP browser extension directly on to the web browser.	- Enable Browser Protection. See: Step 3: Enable Browser Protection in the Intrusion Prevention policy The SEP client modifies the Local Group Policy (GPO) to enforce the browser extension and adds the following key to the registry: Chrome: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForceList Edge: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForceList
Third-party management tools (14.3 RU9 and later)	You do not want the SEP browser extension to override the client user policy on their web browser so that the client user cannot see any other extensions.	- Install the browser extension on the web browser. The most common methods include: Chrome: Chrome Browser Cloud Management See: Set up Chrome Browser Cloud Management Edge: Microsoft Intune See: Configure Microsoft Edge policy settings in Microsoft Intune - Select both the Enable Browser Intrusion Prevention option and the Enable third-party management of extensions option in the SEPM Intrusion Prevention policy. See: Step 3: Enable Browser Protection in the Intrusion Prevention policy
	Your organization uses Active Directory domains.	- Enable Browser Protection. You do not need to enable Enable third-party management of extensions. Step 3: Enable Browser Protection in the Intrusion Prevention policy - Configure the AD Group Policy Object policy to install and manage your browser extensions. You must add the SEP browser extension to your extensions list. SEP then downloads either extension from the Google Web Store. See: Installing the Endpoint Protection Browser Extension for Chrome or Edge using an Active Directory Group Policy Object Note: Items that you configure in the AD GPO policy have the highest priority over any installation method. If you install the SEP client first, the AD GPO policy overwrites the SEP client registry values. If you use the AD GPO policy first and the SEP client installs later, the client skips writing to the registry because it uses the Google Web Store URL.
Add a policy to the registry at: HKEY_CURRENT_USER	You do not want the SEP browser extension to override the client user policy, and you do not want to install and manage browser extensions using a third-party management tool.	- Enable Browser Protection. See: Step 3: Enable Browser Protection in the Intrusion Prevention policy - Add a key to the registry HKEY_CURRENT_USER. See: Installing the Endpoint Protection Browser Extension for Chrome or Edge using the HKEY_CURRENT_USER key

If you upgrade the browser, the extension stays installed.

Step 3: Enable Browser Protection in the Intrusion Prevention policy

You use the Intrusion Prevention policy to enable the SEP browser extension and to install the browser extension directly from the Symantec Endpoint Protection Manager.

NOTE

In 14.3 RU9 or later, you can use a third-party management tool instead of Symantec Endpoint Protection Manager to install the browser extension. If you use a third-party management tool, install the browser extension first and then follow this step.

To enable Browser Protection in the Intrusion Prevention policy

1. Open an Intrusion Prevention policy.
2. On the Intrusion Prevention page, make sure that the following options are checked:
 - **Enable Browser Intrusion Prevention for Windows**
 - **Enable URL reputation**

By default, the **Enable third-party management of extensions** option is cleared.

To install the extension from a third-party management tool and not Symantec Endpoint Protection Manager, check this option. This method removes `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForceList`.

For more information about these settings, see: [Intrusion Prevention settings](#)

3. Click **OK**.

More information

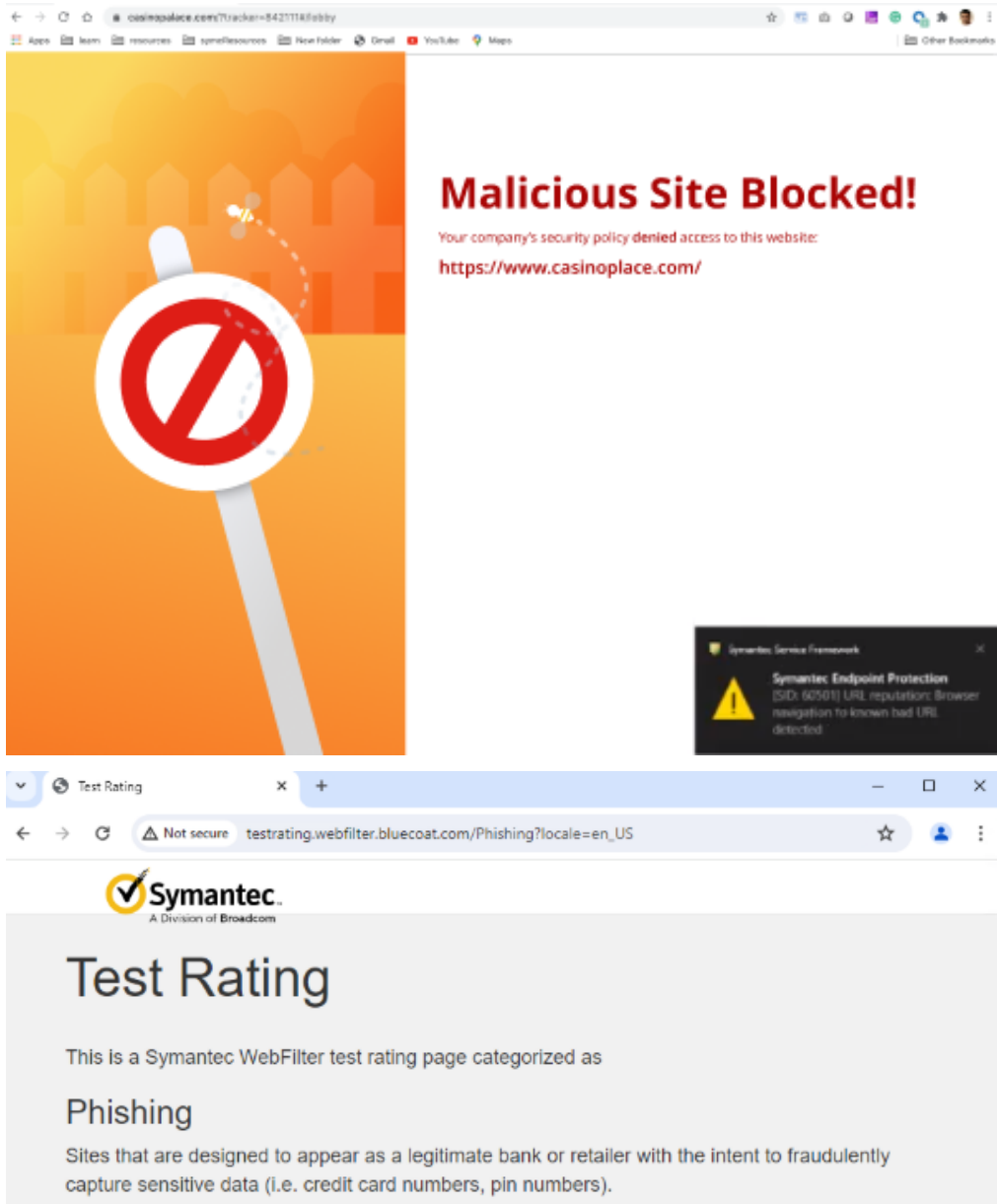
To verify whether the browser extension was installed and enabled correctly, see: [Verify that the browser extension is installed or enabled](#)

For these settings on the cloud console, see: [Managing intrusion prevention in Symantec Endpoint Security](#)

Step 4: Test the SEP browser extension

1. Paste any of the following URLs in a supported web browser to see if the browser blocks them. The browser may take several attempts.
 - http://testrating.webfilter.bluecoat.com/Malicious%20Sources/Malnets?locale=en_US
 - http://testrating.webfilter.bluecoat.com/Malicious%20Outbound%20Data/Botnets?locale=en_US
 - http://testrating.webfilter.bluecoat.com/Phishing?locale=en_US
 - <http://www.fakebook.com>

If Symantec Endpoint Protection detects a malicious URL, you may see one of the following screens, depending on how you configured the browser extension installation.



2. Review the client **Security** log to see if the detections were logged. See:
[Verify the Security log for browser attack detections](#)

(Optional) Verify that the browser extension is installed or enabled

As a troubleshooting step, you can verify that the browser extension is installed on the client computer and the web browser. You can also verify that the browser extension is enabled on both the SEPM and the client computer.

To verify the installation status of the browser extension on the client computer

- In the registry, look for the following items:
 - **Chrome:**
 - HKEY_LOCAL_MACHINE\SOFTWARE\Google\Chrome\NativeMessagingHosts\com.broadcom.webextbridge
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist

(if the **Enable third-party management of extensions** option is cleared [14.3 RU9 or later])

- HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Symantec\Symantec Endpoint Protection\{965393C7-9C7B-4B0A-BB01-CD0BC8425DEB}\Common Client\PathExpansionMap > WebExtDefs\20210721.023
- **Edge:**
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Edge\NativeMessagingHosts\com.broadcom.webextbridge
 - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\ExtensionInstallForcelist (if the **Enable third-party management of extensions** option is cleared [14.3 RU9 or later])
- Verify that the WebExt folder and the updates.xml file exist:
C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.4345.2000.105\Data\Definitions\WebExt\20210221.007\updates.xml
- In the Symantec Endpoint Protection Manager, verify that the browser extension engine and definitions are enabled: Click **Help > Troubleshooting > Versions > Browser Extension Engine** and **Browser Extension**.

To verify the installation status of the browser extension on the web browser

- On the web browser, do the following step:
 - **Chrome:** In the Chrome web browser, click the vertical ellipsis > **Settings > Extensions > Symantec Endpoint Protection > Details**. Look for the **Version** number.
 - **Edge:** In the Microsoft Edge web browser, click the vertical ellipsis > **Extensions > Symantec Extension**.

To verify that the browser extension is enabled

1. On the Symantec Endpoint Protection client, go to the following locations:
 - The client System log displays an event every time that the browser extension is enabled or disabled, installed, or uninstalled, or removed from the browser.
 - **Help > Troubleshooting > Versions > Browser Extension Engine** and **Browser Extension**.
2. In the Symantec Endpoint Protection Manager, go to the following locations:
 - The **Clients** page > **Clients** tab > **Protection technology** view displays whether the browser extensions are enabled or disabled.
 - On the **Home** page, under **Endpoint Status**, select the clients that have the **Disabled** status, and click **Details**. In the report, view the browser extensions that are enabled or disabled. Click **Save** to save the report in HTML format.

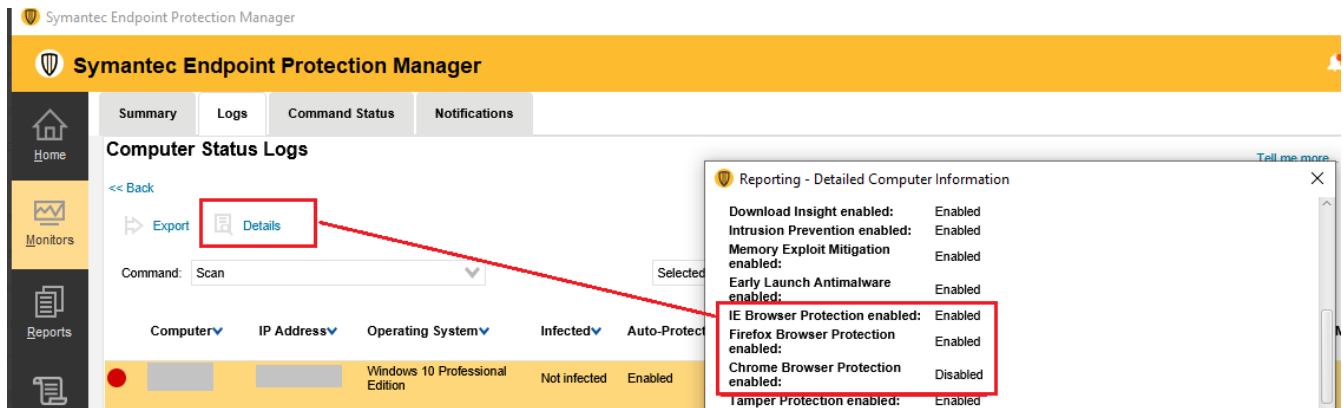
The screenshot shows the Symantec Endpoint Protection Manager interface. On the left, the 'Endpoint Status' section displays a donut chart with the following data: 1 Up-to-date (green), 0 Out-of-date (yellow), 0 Offline (blue), 1 Disabled (red), and 0 Host Integrity Failed (orange). A 'View Details' link is present. The main area shows a table of endpoints. The first row is highlighted, showing a 'Disabled' status. The 'Browser Intrusion Prevention Chrome Status' column is highlighted in red.

Computer Name	Operating System	Group	User Name	Last Scan Time	IP Address	Auto-protect Status	Unit Enabled Status	Firewall Status	SONAR Status	Download Insight Status	Network Intrusion Prevention Status	Browser Intrusion Prevention IE Status	Browser Intrusion Prevention Firefox Status	Browser Intrusion Prevention Chrome Status
DESKTOP-...	Windows 10 Professional Edition	My Company	admin	05/18/2021 17:55:42	05/18/2021 17:45:01	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Disabled

NOTE

The reports show a single status for both the Chrome and Edge extensions. If only one extension is installed or malfunctioning, the status appears as enabled or a malfunction.

- On the **Home** page under **Favorite Reports**, the **Symantec Endpoint Protection Weekly Status** report displays which clients have the extensions on or off.
- On the **Reports > Quick Reports > Computer Status** report type > **Protection Content Versions** report, click **Create Report**. Click the **Security Status Summary** report to see which clients have a disabled or malfunctioning browser extension, or updated browser extensions definitions.
- On the **Monitors > Logs** page, the **Computer Status** log displays a column for **Chrome Browser Protection Enabled**. Click **Details** for the revision number for **Browser Extensions Definitions**. Use this information to make sure the browser extension content is downloaded to the client.



(Optional) Review the Security log for browser attack detections

To view specific browser attack detections, review the Symantec Endpoint Protection Security log. For example, see the following entries or notifications:

- Symantec Endpoint Protection [SID: 60501] URL Reputation Browser navigation to known bad URL blocked. `<path>`
- System Infected: PlugX Remote Access Tool Activity 2 attack blocked for this application: `<path>`
- [SID: 29565] Web Attack: Webpulse Bad Reputation Domain Request attack blocked. Traffic has been blocked for this application: `<path>`

Browser extension FAQs

Q: What are the browser versions that Browser Protection on Windows clients supports?

- *Microsoft Edge*: The latest release and two releases prior.
- *Google Chrome*: The latest release and two releases prior.

For information about which versions of which browsers are supported, see: [Supported browsers for Browser Intrusion Prevention in Endpoint Protection](#)

Q: Do browser extensions use definitions?

Browser attack detections require Browser Extension definitions, SymPlatform definitions, and IPS definitions that Symantec LiveUpdate downloads. See:

[About the types of content that LiveUpdate downloads](#)

Q: Which IPS signatures are used for URL reputation detections?

-
- SID 60501 detections are for browser-based detections.
 - SID 29565 detections are triggered from non-browser sources.

Q: How do I disable or uninstall the Chrome or Edge browser extension?

You should always keep the browser extensions installed and enabled for protection. However, if you must troubleshoot issues with the browser, you can disable or uninstall the browser extension.

You can disable the browser extension by unchecking **Enable Browser Intrusion Prevention for Windows** in the Intrusion Prevention policy. Disabling this option unloads the Chrome browser extension or Microsoft Edge extension that is installed on client computers. Re-enabling these options reloads the extension. It might take some time for the extension to reload.

The WebExt features such as the WebFilter and scanner are disabled, but remain installed. If you disable any part of the WebExt feature, it disables protection for the entire feature.

You can uninstall the Chrome or Edge browser extension in the following ways:

- Disable the IPS policy, which uninstalls extensions from all browsers.
- Uninstall the browser extension by removing the Google Chrome entry or Microsoft Edge entry from the AD GPO policy. In 14.3 RU9 or later, uninstall the extension if it is installed by a third-party management tool.
- Uninstall the SEP client.
- Reinstall the SEP client without the Intrusion Prevention component.
- Run CleanWipe. CleanWipe uninstalls both the Symantec Endpoint Protection client and either browser extension.

Troubleshooting and known issues

You can run the Symantec Diagnostic (SymDiag) tool to collect the following information about the browser extension:

- The .SDBZ file. SymDiag takes a snapshot of your computer and logs the data in one file with an .SDBZ filename extension.
- Information about unexpected detections in the WPP log.

To start SymDiag, in the client, click **Help > Download Symantec Diagnostic Tool**. See:

For more information about how to troubleshoot issues with the browser extension, see:

[Using SymDiag to collect data for support cases](#)

Known issues

- The following list shows the most common issues that you might encounter when you install and use a browser extension. To allow the unmanaged client to access the entire website, add the blocked domain to the list of trusted hosts. See:
[About excluding items from scans](#)
- If an unmanaged client detects a malicious URL, the Edge extension blocks the entire website. The Chrome extension blocks just the malicious URL.
- If you use third-party developer tools and you block native messaging, the SEP browser extension shows that it is installed but not functioning. To solve this issue, add the following key to the registry:

```
HKEY_CURRENT_USER\Software\Policies\Google\Chrome\NativeMessagingAllowlist 1 =  
'com.broadcom.webextbridge'  
HKEY_CURRENT_USER\Software\Policies\Microsoft\Edge\NativeMessagingAllowlist 1 =  
'com.broadcom.webextbridge'
```

More information

Chrome: [NativeMessagingBlocklist](#)

Edge: [Microsoft Policies - NativeMessagingBlocklist](#)

[CRE-17244]

- When Symantec Endpoint Protection Manager installs the extensions for Chrome and Edge browsers, it tracks the successes and failures on each endpoint. If the **Enable third-party management of extensions** option is enabled and you use a third-party tool to install the extensions, Symantec Endpoint Protection Manager may not be able to detect if the installation failed. Instead, the extension mistakenly shows that it installed successfully. This issue will be addressed in a future release. [INFODEVSEP-74]
- If the Chrome Incognito mode is enabled (disabled by default), the client does not block malicious URLs. To disable this mode in the Google Chrome web browser, click the vertical ellipsis > **Settings** > **Extensions** > **Symantec Endpoint Protection** > **Details**, and turn off **Allow in Incognito**.
- If you add a Trusted Web Domain Exception URL using an IPv4 or IPv6 address, the Chrome extension does not recognize the address.
- When you stop the client service, the Chrome browser extension still runs, but the client does not generate an event in the Security log.
- As the Symantec Endpoint Protection client starts, the web extension runs. However, there is a short time period when the client does not generate any notifications or logs for an allowed or blocked URL. [MI-4947]

Setting up a list of excluded computers

Excluded hosts are supported for network intrusion prevention and the firewall.

You can set up a list of computers for which the client does not match attack signatures or check for port scans or denial-of-service attacks. Network intrusion prevention and peer-to-peer authentication allow any source traffic from hosts in the excluded hosts list. However, network intrusion prevention and peer-to-peer authentication continue to evaluate any destination traffic to hosts in the list. The list applies to both inbound traffic and outbound traffic, but only to the source of the traffic. The list also applies only to remote IP addresses.

For example, you might exclude computers to allow an Internet service provider to scan the ports in your network to ensure compliance with their service agreements. Or, you might have some computers in your internal network that you want to set up for testing purposes.

NOTE

You can also set up a list of computers that allows all inbound traffic and outbound traffic unless an IPS signature detects an attack. In this case, you create a firewall rule that allows all hosts.

To set up a list of excluded computers

1. In the console, open an Intrusion Prevention policy.
2. On the policy page, click **Intrusion Prevention**.
3. If not checked already, check **Enable excluded hosts** and then click **Excluded Hosts**.
4. In the **Excluded Hosts** dialog box, check **Enabled** next to any host group that you want to exclude from network intrusion prevention. See:

[Blocking traffic to or from a specific server](#)

5. To add the hosts that you want to exclude, click **Add**.
6. In the **Host** dialog box, in the drop-down list, select one of the following host types:
 - IP address
 - IP range
 - Subnet
7. Enter the appropriate information that is associated with the host type you selected.

For more information about these options, click **Help**.

-
8. Click **OK**.
 9. Repeat step 5 and click **OK** to add additional devices and computers to the list of excluded computers.
 10. To edit or delete any of the excluded hosts, select a row, and then click **Edit** or **Delete**.
 11. Click **OK**.
 12. When you finish configuring the policy, click **OK**.

Configuring client notifications for intrusion prevention and Memory Exploit Mitigation

By default, notifications appear on client computers when the client detects intrusion protection events and Memory Exploit Mitigation. When these notifications are enabled, they display a standard message. For IPS notifications, you can add customized text to the standard message.

To configure client notifications for intrusion prevention and Memory Exploit Mitigation

1. In the console, click **Clients** and under **Clients**, select a group.
2. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
3. To the right of **Client User Interface Control Settings**, click **Tasks**, and then click **Edit Settings**.
4. In the **Client User Interface Control Settings for group name** dialog box, click either **Server control** or **Mixed control**.
5. Beside **Mixed control** or **Server control**, click **Customize**.
If you click **Mixed control**, on the **Client/Server Control Settings** tab, beside **Show/Hide Intrusion Prevention notifications**, click **Server**. Then click the **Client User Interface Settings** tab.
6. In the **Client User Interface Settings** dialog box or tab, click **Display Intrusion Prevention and Memory Exploit Mitigation notifications**.
7. To enable a sound when the notification appears, click **Use sound when notifying users**.
8. Click **OK**.
9. Click **OK**.

More information

- [Managing intrusion prevention](#)
- [Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)
- [Setting up administrator notifications](#)

About Symantec IPS signatures

Symantec intrusion prevention signatures are installed on the client by default.

Intrusion prevention uses the Symantec signatures to monitor individual packets or streams of packets. For streams of packets, intrusion prevention can remember the list of patterns or partial patterns from previous packets. It can then apply this information to subsequent packet inspections.

Symantec signatures are downloaded to the client as part of LiveUpdate content. For Mac computers, there are some additional network intrusion prevention signatures that are built into the software.

NOTE

Symantec creates the signatures based on their own research or public information.

On Windows computers, LiveUpdate content also includes signatures for browser intrusion prevention.

Network intrusion prevention signatures	Network signatures match patterns of an attack that can crash applications or exploit the operating systems on your client computers. You can change whether a Symantec network signature blocks or allows traffic. You can also change whether Symantec Endpoint Protection logs a detection from a signature in the Security log.
Browser protection signatures (Windows only) (Browser intrusion prevention)	Browser signatures match patterns of attack on supported browsers, such as script files that can crash the browser. You cannot customize the action or log setting for browser signatures, but you can exclude a browser signature. You can configure browser protection to log the browser detections but not block them. This action helps you identify those browser signatures that you may need to exclude. After you create the signature exclusions, you disable log-only mode.

The Symantec Security Response team supplies the attack signatures. The intrusion prevention engine and the corresponding set of signatures are installed on the client by default. The signatures are part of the content that you update on the client.

More information

- For the Symantec database of attack signatures, see: [Attack Signatures](#)
- For information on Symantec IPS signatures for Microsoft vulnerabilities, see: [Symantec Endpoint Response to Microsoft Monthly Security Bulletins](#)
- For information about the built-in IPS signatures for Mac clients, see: [Built-in signatures for Symantec Endpoint Protection IPS for Mac](#)
- [Creating exceptions for IPS signatures](#)

Creating exceptions for IPS signatures

You use exceptions to change the behavior of Symantec IPS signatures.

For Windows and Mac computers, you can change the action that the client takes when the IPS recognizes a network signature. You can also change whether the client logs the event in the Security log.

For Windows computers, you cannot change the behavior of Symantec browser signatures; unlike network signatures, browser signatures do not allow custom action and logging settings. However, you can create an exception for a browser signature so that clients ignore the signature.

NOTE

When you add a browser signature exception, Symantec Endpoint Protection Manager includes the signature in the exceptions list and automatically sets the action to **Allow** and the log setting to **Do Not Log**. You cannot customize the action or the log setting.

For more information, see:

[Managing intrusion prevention](#)

NOTE

To change the behavior of a custom IPS signature that you create or import, you edit the signature directly. Custom signatures are supported on Windows computers only.

To create an exception for IPS signatures

-
1. In the console, open an Intrusion Prevention policy.
 2. Under **Windows Settings** or **Mac Settings**, click **Exceptions**, and then click **Add**.

NOTE

The signatures list populates with the latest LiveUpdate content that the management console downloaded. For Windows computers, the list appears blank if the management server has not yet downloaded the content. For Mac computers, the list always contains at least the built-in signatures, which are installed automatically on your Mac clients.

3. In the **Add Intrusion Prevention Exceptions** dialog box, do the following actions to filter the signatures:
 - (Windows only) To display only the signatures in a particular category, select an option from the **Show category** drop-down list. If you select **Browser Protection**, the signature action options automatically change to **Allow** and **Do Not Log**.
 - (Windows and Mac) To display the signatures that are classified with a particular severity, select an option from the **Show severity** drop-down list.
4. Select one or more signatures.

To make the behavior for all signatures the same, click **Select All**.
5. Click **Next**.
6. In the **Signature Action** dialog box, set the following options and then click **OK**.
 - Set **Action** to **Block** or **Allow**
 - Set **Log** to **Log the traffic** or **Do not log the traffic**.

NOTE

These options only apply to network signatures. For browser signatures, click **OK**.

If you want to revert the signature's behavior back to the original behavior, select the signature in the **Exceptions** list, and then click **Delete**.

7. Click **OK** to save the policy changes.

More information

[Managing exceptions in Symantec Endpoint Protection](#)

Managing custom intrusion prevention signatures

You can write your own network intrusion prevention signatures to identify a specific intrusion and reduce the possibility of signatures that cause a false positive. The more information you can add to a custom signature, the more effective the signature is.

WARNING

You should be familiar with the TCP, UDP, or ICMP protocols before you develop intrusion prevention signatures. An incorrectly formed signature can corrupt the custom signature library and damage the integrity of the clients.

NOTE

You must have the firewall installed and enabled to use custom IPS signatures. See:

[Choosing which security features to install on the client](#)

Table 81: Managing custom intrusion prevention signatures

Task	Description
Create a custom library with a signature group	You must create a custom library to contain your custom signatures. When you create a custom library, you use signature groups to manage the signatures more easily. You must add at least one signature group to a custom signature library before you add the signatures. See: • About custom IPS signatures • Creating a custom IPS library
Add custom IPS signatures to a custom library	You add custom IPS signatures to a signature group in a custom library. See: Adding signatures to a custom IPS library
Assign libraries to client groups	You assign custom libraries to client groups rather than to a location. See: Assigning multiple custom IPS libraries to a group
Change the order of signatures	Intrusion prevention uses the first rule match. Symantec Endpoint Protection checks the signatures in the order that they are listed in the signatures list. For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures: • Block all traffic on port 80. • Allow all traffic on port 80. If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed. Note: Firewall rules take precedence over intrusion prevention signatures. For more information, see: Changing the order of custom IPS signatures
Copy and paste signatures	You can copy and paste signatures between groups and between libraries.
Define variables for signatures	When you add a custom signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library. See: Defining variables for custom IPS signatures
Test custom signatures	You should test the custom intrusion prevention signatures to make sure that they work. See: Testing custom IPS signatures

About custom IPS signatures

You can create your own IPS network signatures. These signatures are packet-based.

Unlike Symantec signatures, custom signatures scan single packet payloads only. However, custom signatures can detect attacks in the TCP/IP stack earlier than the Symantec signatures.

Packet-based signatures examine a single packet that matches a rule. The rule is based on various criteria, such as port, protocol, source or destination IP address, TCP flag number, or an application. For example, a custom signature can monitor the packets of information that are received for the string “phf” in GET / cgi-bin/phf? as an indicator of a CGI program attack. Each packet is evaluated for that specific pattern. If the packet of traffic matches the rule, the client allows or blocks the packet.

You can specify whether or not Symantec Endpoint Protection logs a detection from custom signatures in the Packet log.

NOTE

You must have the firewall installed and enabled to use custom IPS signatures. See:

[Choosing which security features to install on the client](#)

Custom signatures are supported on Windows computers only. See:

Creating a custom IPS library

You create a custom IPS library to contain your custom IPS signatures. See:

[Managing custom intrusion prevention signatures](#)

To create a custom IPS library

1. In the console, on the **Policies** page, under **Policies**, click **Intrusion Prevention**.
2. Click the **Custom Intrusion Prevention** tab.
3. Under **Tasks**, click **Add Custom Intrusion Prevention Signatures**.
4. In the **Custom Intrusion Prevention Signatures** dialog box, type a name and optional description for the library.
The NetBIOS Group is a sample signature group with one sample signature. You can edit the existing group or add a new group.
5. To add a new group, on the **Signatures** tab, under the **Signature Groups** list, click **Add**.
6. In the **Intrusion Prevention Signature Group** dialog box, type a group name and optional description, and then click **OK**.
The group is enabled by default. If the signature group is enabled, all signatures within the group are enabled automatically. To retain the group for reference but to disable it, uncheck **Enable this group**.
7. Add a custom signature. See:

[Adding signatures to a custom IPS library](#)

Adding signatures to a custom IPS library

You add custom intrusion prevention signatures to a new or existing custom IPS library. See:

[Managing custom intrusion prevention signatures](#)

To add a custom signature

1. Create a custom IPS library. See:
[Creating a custom IPS library](#)
2. On the **Signatures** tab, under **Signatures for this Group**, click **Add**.
3. In the **Add Signature** dialog box, type a name and optional description for the signature.
4. In the **Severity** drop-down list, select a severity level.
Events that match the signature conditions are logged with this severity.

5. In the **Direction** drop-down list, specify the traffic direction that you want the signature to check.
6. In the **Content** field, type the syntax of the signature.

For example, signatures for some common protocols use the following syntax:

HTTP	<pre>rule tcp, dest=(80,443), saddr=\$LOCALHOST, msg="MP3 GET in HTTP detected", regexcontent="[Gg][Ee][Tt] .*[Mm][Pp]3 ."</pre>
FTP	<pre>rule tcp, dest=(21), tcp_flag&ack, saddr=\$LOCALHOST, msg="MP3 GET in FTP detected", regexcontent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"</pre>

For more information about the syntax, click **Help**. See:

[Syntax for custom intrusion prevention signatures](#)

7. If you want an application to trigger the signature, click **Add**.
8. In the **Add Application** dialog box, type the file name and an optional description for the application.
For example, to add the application Internet Explorer, type the file name as `iexplore` or `iexplore.exe`. If you do not specify a file name, any application can trigger the signature.
9. Click **OK**.
The added application is enabled by default. If you want to disable the application until a later time, uncheck the check box in the **Enabled** column.
10. In the **Action** group box, select the action you want the client to take when the signature detects the event:

Block	Identifies and blocks the event or attack and records it in the Security Log
Allow	Identifies and allows the event or attack and records it in the Security Log

11. To record the event or attack in the Packet Log, check **Write to Packet Log**.

12. Click **OK**.

The added signature is enabled by default. If you want to disable the signature until a later time, uncheck the check box in the **Enabled** column.

13. You can add additional signatures. When you are finished, click **OK**.

14. If you are prompted, assign the custom IPS signatures to a group.

You can also assign multiple custom IPS libraries to a group. See:

[Assigning multiple custom IPS libraries to a group](#)

Changing the order of custom IPS signatures

The IPS engine for custom signatures checks the signatures in the order that they are listed in the signatures list. Only one signature is triggered per packet. When a signature matches an inbound traffic packet or outbound traffic packet, the IPS engine stops checking other signatures. So that the IPS engine executes signatures in the correct order, you can change the order of the signatures in the signatures list. If multiple signatures match, move the higher priority signatures to the top.

For example, if you add a signature group to block TCP traffic in both directions on destination port 80, you might add the following signatures:

-
- Block all traffic on port 80.
 - Allow all traffic on port 80.

If the Block all traffic signature is listed first, the Allow all traffic signature is never enacted. If the Allow all traffic signature is listed first, the Block all traffic signature is never enacted, and all HTTP traffic is always allowed.

NOTE

Firewall rules take precedence over intrusion prevention signatures.

For more information, see:

[Managing custom intrusion prevention signatures](#)

To change the order of custom IPS signatures

1. Open a custom IPS library.
2. On the **Signatures** tab, in the **Signatures for this Group** table, select the signature that you want to move, and then do one of the following actions:
 - To process this signature before the signature above it, click **Move Up**.
 - To process this signature after the signature below it, click **Move Down**.
3. When you finish configuring this library, click **OK**.

Defining variables for custom IPS signatures

When you add a custom IPS signature, you can use variables to represent changeable data in signatures. If the data changes, you can edit the variable instead of editing the signatures throughout the library. See:

[Managing custom intrusion prevention signatures](#)

Before you can use the variables in the signature, you must define them. The variables that you define in the custom signature library can then be used in any signature in that library.

You can copy and paste the content from the existing sample variable to start as a basis for creating content.

To define variables for custom IPS signatures

1. Create a custom IPS library.
[Creating a custom IPS library](#)
2. In the **Custom Intrusion Prevention Signatures** dialog box, click the **Variables** tab.
3. Click **Add**.
4. In the **Add Variable** dialog box, type a name and optional description for the variable.
5. Add a content string for the variable value of up to 255 characters.
When you enter the variable content string, follow the same syntax guidelines that you use for entering values into signature content.
[Syntax for custom intrusion prevention signatures](#)
6. Click **OK**.
After the variable is added to the table, you can use the variable in any signature in the custom library.

To use variables in custom IPS signatures

1. On the **Signatures** tab, add or edit a signature.
2. In the **Add Signature** or **Edit Signature** dialog box, in the **Content** field, type the variable name with a dollar sign (\$) in front of it.
For example, if you create a variable named HTTP for specifying HTTP ports, type the following:
\$HTTP

3. Click **OK**.
4. When you finish configuring this library, click **OK**.

Assigning multiple custom IPS libraries to a group

After you create a custom IPS library, you assign it to a group rather than an individual location. You can later assign additional custom IPS libraries to the group. See:

[Managing custom intrusion prevention signatures](#)

To assign multiple custom IPS libraries to a group

1. In the console, click **Clients**.
2. Under **Clients**, select the group to which you want to assign the custom signatures.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, click **Custom Intrusion Prevention**.
4. In the **Custom Intrusion Prevention for group name** dialog box, check the check box in the **Enabled** column for each custom IPS library you want to assign to that group.
5. Click **OK**.

Testing custom IPS signatures

After you create custom IPS signatures, you should test them to make sure that they function correctly.

Table 82: Testing custom IPS signatures

Step	Description
Step 1: Make sure that clients use the current policy	The next time that the client receives the policy, the client applies the new custom signatures. See: Updating client policies
Step 2: Test the signature content on the client	You should test the traffic that you want to block on the client computers. For example, if your custom IPS signatures should block MP3 files, try to download some MP3 files to the client computers. If the download does not occur, or times out after many tries, the custom IPS signature is successful. You can click Help for more information about the syntax that you can use in custom IPS signatures. See: Syntax for custom intrusion prevention signatures
Step 3: View blocked events in Symantec Endpoint Protection Manager	You can view events in the Network and Host Exploit Mitigation Attack logs. The message you specify in the custom IPS signature appears in the log. See: Monitoring the Symantec Endpoint Protection clients

More information

[Managing custom intrusion prevention signatures](#)

Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy

Refer to the following sections for more information:

-
- [How does Memory Exploit Mitigation protect applications?](#)
 - [Types of exploit protection](#)
 - [Memory Exploit Mitigation requirements](#)
 - [Correcting and preventing false positives](#)
 - [Finding the logs and reports for Memory Exploit Mitigation events](#)
 - [Auditing protection for a terminated the application](#)

How does Memory Exploit Mitigation protect applications?

Symantec Endpoint Protection includes Memory Exploit Mitigation, which uses multiple mitigation techniques to stop exploit attempts against both known and unknown vulnerabilities in the software. For example, when the client user runs an application such as Internet Explorer, an exploit might instead launch a different application that contains malicious code.

To stop an exploit, Memory Exploit Mitigation injects a DLL into a protected application. After Memory Exploit Mitigation detects the exploit attempt, it either blocks the exploit or terminates the application that the exploit threatens. Symantec Endpoint Protection displays a notification to the user on the client computer about the detection, and logs the event in the client's Security log.

For example, the client user might see the following notification:

Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected. Symantec Endpoint Protection will terminate <application name> application

Memory Exploit Mitigation continues to block the exploit or terminate the application until the client computer runs a version of the software where the vulnerability is fixed.

Types of exploit protection

Memory Exploit Mitigation uses multiple types of mitigation techniques to handle the exploit, depending on which technique is most appropriate for the type of application. For example, both the StackPvt and RopHeap techniques block the exploits that attack Internet Explorer. See:

[Symantec Endpoint Protection Memory Exploit Mitigation techniques](#)

NOTE

If you have enabled the Microsoft App-V feature on your computers, Memory Exploit Mitigation does not protect the Microsoft Office processes that App-V protects.

Memory Exploit Mitigation requirements

Memory Exploit Mitigation is only available if you have installed intrusion prevention. Memory Exploit Mitigation has its own set of separate signatures that is downloaded along with the intrusion prevention definitions. However, you can enable or disable intrusion prevention and Memory Exploit Mitigation independently.

In addition, you must run LiveUpdate at least once for the list of applications to appear in the Memory Exploit Mitigation policy. By default, protection is enabled for all applications that appear in the policy. See:

[Checking that Symantec Endpoint Protection Manager has the latest content](#)

Correcting and preventing false positives

Occasionally, Memory Exploit Mitigation may unintentionally terminate an application on the client computer. If you determine that an application's behavior is legitimate and was not exploited, the detection is a false positive. For false positives, you should disable protection until Symantec Security Response changes the Memory Exploit Mitigation behavior.

The following table displays the steps to handle false positive detections.

Table 83: Steps to find and remediate a false positive

Tasks	
Step 1: Find out which applications terminate unexpectedly on the client computers.	You can find out which applications were terminated on the client computer in the following ways: • A user on the client computer notifies you that an application does not run. • Open the Memory Exploit Mitigation log or report that lists which mitigation technique terminated the applications on the client computer. Note: Sometimes the mitigation techniques do not produce logs due to the nature of the exploit. For more information, see: Finding the logs and reports for Memory Exploit Mitigation events
Step 2: Disable protection and audit the techniques that terminate the application.	Disable protection at the most minimal level first so that other processes remain protected. Do not turn off Memory Exploit Mitigation to allow the application to run until you have tried all other methods. After each of the following subtasks, go to Step 3. 1. First, audit the protection for the specific application that the mitigation technique terminated. For example, if Mozilla Firefox was terminated, you would disable either the SEHOP technique or the HeapSpray technique. Sometimes a mitigation technique does not create log events due to the nature of the exploit, so you cannot be sure which mitigation technique terminated the application. In this case, you should disable each technique that protects that application, one at a time, until you find which technique caused the termination. 2. Audit protection for all applications that a single mitigation technique protects. 3. Audit protection for all applications, regardless of the technique. This option is similar to disabling Memory Exploit Mitigation, except that the management server collects the log events for detections. For more information, see: Auditing protection for the mitigation techniques that terminated the application
Step 3: Update the policy on the client computer, and rerun the application.	• If the application runs correctly, the detection for that mitigation technique is a false positive. • If the application does not run the way you expect it to, the detection is a true positive. • If the application still terminates, audit at a level restrictive level. For example, audit a different mitigation technique or for all applications that the technique protects. For more information, see: Updating security policies on the Windows client
Step 4: Report the false positives and reen able protection for the true positives.	For false positive detections: 1. Notify the Symantec team that the detection was a false positive. See: Symantec Insider Tip: Successful Submissions! 2. Keep protection disabled for the terminated application by setting each technique's action to No. 3. After Security Response resolves the issue, reen able protection by changing the technique's action to Yes. For true positive detections: 1. Reenable protection by changing the rule's action for that mitigation technique back to Yes. 2. Check whether there is a patched version or a newer release of the infected application that fixes the current vulnerability. After you install the patched application, rerun it on the client computer to see if Memory Exploit Mitigation still terminates the application.

Finding the logs and reports for Memory Exploit Mitigation events

You need to view the logs and run quick reports to find the applications that Memory Exploit Mitigation terminated.

To find the logs and reports for Memory Exploit Mitigation events

1. In the console, do one of the following actions:

-
- For logs, click **Monitors > Logs > Network and Host Exploit Mitigation** log type > **Memory Exploit Mitigation** log content > **View Log**.

Look for the **Memory Exploit Mitigation Blocked Event** event type. The **Event type** column lists the mitigation technique, and the **Action** column lists whether or not the application in the **Application Name** column was blocked. For example, the following log event indicates a Stack Pivot attack:

Attack: Return Oriented Programming Changes Stack Pointer

- For quick reports, click **Reports > Quick Reports > Network and Host Exploit Mitigation** report type > **Memory Exploit Mitigation Detections** report > **Create Report**.

Look for the blocked Memory Exploit Mitigation detections.

Auditing protection for a terminated application

When you test for false positives, change the Memory Exploit Mitigation behavior so that it audits a detection, but lets the application run. However, Memory Exploit Mitigation does not protect the application.

To audit protection for a terminated application

1. In the console, click **Policies > Memory Exploit Mitigation > Memory Exploit Mitigation**.
2. On the **Mitigation Techniques** tab, next to **Choose a mitigation technique**, select the technique that terminated the application, such as **StackPvt**.
3. Under the **Protected** column, select the terminated application, and then change **Default (Yes)** to **Log Only**.
Change the action to **No** after you verified that the detection is a true false positive. Both **Log Only** and **No** allow the possible exploit, but also let the application run.
Some applications have multiple mitigation techniques that block the exploit, so follow this step for each technique individually.
4. (Optional) Do one of the following steps, and then click **OK**:
 - If you are not sure which technique terminated the application, click **Choose a protection action for all applications for this technique**. This option overrides the settings for each technique.
 - If you have a mix of 14.0.1 clients and legacy 14 MPx clients, and you only want to test the 14.0.1 clients, click **Set the protection action for all techniques to log only**.
5. (Optional) To test the application regardless of technique, on the **Application Rules** tab, in the **Protected** column, uncheck the terminated application, and then click **OK**.
For legacy 14 MPx clients, you can only use this option. After you upgrade to version 14.0.1 clients, reenabling protection and doing the finer grained tuning. Open the **Computer Status** log to find which clients run which product version.
6. In the console, click **Policies > Memory Exploit Mitigation**.
7. Uncheck **Enable Memory Exploit Mitigation**.
8. Click **OK**.
9. In the Symantec Endpoint Protection Manager, make sure that Symantec Insight is enabled. Insight is enabled by default. See:
[Customizing Download Insight settings](#)
10. Download and run the SymDiag tool on the client computer. See:
[Download SymDiag to detect product issues](#)
11. On the SymDiag tool **Home** page, click **Collect Data for Support**, and for the **Debug logging > Advanced** option, set the **WPP Debug > Trace Level** to **Verbose**. See:
[Advanced debug log options in SymDiag for Endpoint Protection clients](#)
12. Reproduce the false positive detection.
13. After the log collection finishes, submit the `.sdbz` file by opening a new case or updating an existing case with this new information. Submit to:
[Create or update support cases with data collected by SymDiag](#)

14. Submit the detected application to the [SymSubmit site](https://symsubmit.symantec.com). For instructions on how to submit a false positive or false negative. See:

[Symantec Insider Tip: Successful Submissions!](#)

https://symsubmit.symantec.com

Symantec Submission

Not Detected by Symantec Incorrectly Detected by Symantec

Use the form below to tell us about a situation where you believe that a Symantec product has incorrectly detected a file. This is also called a **False Positive**.

Submission Details

Submission Type *

-- Please Select --

-- Please Select --

File Submission

Upload a File

Provide an MD5 or SHA-256 hash of a file

Provide Direct Download URL

Provide a password protected URL

Provide blocked file URL (CMA / WSSMA Service)

URL Submission

Provide blocked URL (IPS)

Provide Blocked URL (SEP Mobile for IOS/ProxySG/Webpulse)

Provide Dynamic Adversary Intelligence URL (ATP)

Website Submission

Provide False Positive Malicious / Phish Web Page (Safe Web)

Provide False Positive Scam Insight Web Page (Safe Web)

- For the **Additional details** textbox, type when the detection occurred and the product. For example, type the **B2 Symantec Endpoint Protection 14.x** product, and click the **C5 - IPS** event.
- Provide the Technical Support case number from the previous step, the application that triggered the MEM detection, and details about the application's version number.

For example, you might add: "Blocked Attack: Return Oriented Programming API Invocation attack against C:\Program Files\VideoLAN\VLC\vlc.exe", the version for vlc.exe is 2.2.0-git-20131212-0038. This is not the latest available version but it is the version that our organization is required to use."

15. On the client computer, compress a copy of the submissions folder that is located at: %PROGRAMDATA%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK.

Submit this folder to Technical Support and notify them of the tracking number for the false positive submission that you opened in the previous step. Technical Support ensures that all necessary logs and materials are intact and associated with the false positive investigation.

Symantec Endpoint Protection Memory Exploit Mitigation techniques

Memory Exploit Mitigation (MEM) stops exploit attempts against both known and unknown vulnerabilities on software on your Windows client computers. MEM uses the following types of mitigation techniques to stop these attacks:

- **SEHOP** (Structured exception handling overwrite protection) (14)
Memory Exploit Mitigation provides structured exception handling overwrite protection for applications such as the RealPlayer media player. An exploit attack can control the execution flow of software toward the attacker's shellcode by using an overwrite exception handler function. The exception handler function address is stored in stack memory and can easily be overwritten when a stack buffer overflow exists. Windows operating systems include SEHOP, but some Windows Vista operating systems disable SEHOP by default. Memory Exploit Mitigation provides protection even if SEHOP in Windows is turned off. SEHOP attacks occur on 32-bit clients only.
- **Java Security Manager**
Memory Exploit Mitigation blocks Java Applets that try to disable Windows Security Manager. Some exploit attacks use a Java Applet to turn off Security Manager to allow Java code to execute privileged actions.
- **StackPvt (StackPivot)**
The Stack Pivot technique detects if the call stack address changed. This event indicates the exploit changed the stack pointer (ESP) register to point to the exploit's fake or crafted call stack memory. The fake memory contains the ROP attack chains.
- **ForceDEP** (Force Data Execution Prevention)
Exploit attacks usually insert their malicious executable code (called shellcode) into the stack memory (using the buffer overflow) or heap memory (using heap spraying). The exploit then hijacks the flow of execution towards these locations. To mitigate this attack, Windows XP SP2 and later includes data execution prevention (DEP), a system-level protection that marks these memory locations as non-executable. However, the problem is that this feature can be turned off using a `SetProcessDEPPolicy()` API call. Additionally, for a process to be protected with DEP, it should be compiled with the `/NXCOMPAT` switch. The **ForceDEP** technique prevents DEP from being turned off, even on those programs that are not compiled with that switch.
- **ForceASLR** (Force address space layout randomization)
For an exploit to modify or damage the operating system, it needs to call system APIs, such as `URLDownloadToFile` and `CreateProcess`. In early Windows XP and earlier, system DLLs such as `Kernel32.dll` were always loaded to fixed and predictable memory locations. Therefore, hard-coded addresses easily called APIs. Additionally, after DEP was introduced, exploits have invented alternative method to execute code called return-oriented programming (ROP). Rather than write and execute shellcode in stack or heap memory, the shellcode is instead constructed using a combination of existing executable code bytes from various DLLs loaded in the process. To prevent this process, Windows Vista and later versions introduced ASLR. This feature randomizes the load address of DLLs in the memory, which makes hard-coded address use ineffective. However, for a DLL to be loaded in random memory it should have been compiled with `/DYNAMICBASE` switch. Some old DLLs are still compiled without this switch, which exploits can take advantage of. **ForceASLR** makes the ASLR mandatory on those DLLs.
- **HeapSpray**
A heap spray attack occurs when the attacker tries to place its attack code to a predetermined memory location. The HeapSpray technique reserves the commonly used memory locations to prevent an attacker from using them. Heap spray attacks are a type of buffer attack that is seen in older web browsers and applications.
- **EnhASLR** (Enhance Address space layout randomization) (14.0.1)
The EnhASLR technique allocates random memory regions in a process. The allocation of memory becomes less predictable, which helps to mitigate heap spraying. EnhASLR also increases entropy for ASLR and DLL relocations.
- **NullProt** (Null Page Protection) (14.0.1)
NULL (0x00000000) is a valid memory address that an exploit may take advantage of. The NullProt technique pre-allocates this memory location to avoid its potential use.
- **DIILoad** (14.0.1)
Prevents a process from loading a DLL from a shared folder. Some exploits uses this vector to execute DLL directly from their malicious servers, such as `\\malicious.com\\malware.dll`. Note that the DIILoad technique does

not prevent remote loading of DLL's over local networks such as the localhost, link local, and private IP addresses. Between the time the load path is checked and the actual loading, the result of querying the DNS server for a remote path with a host name might be different.

The following mitigation techniques protect against return-oriented programming (ROP) attacks:

- **StackNX** (14.0.1)
The StackNX technique prevents call to memory protection APIs such as `VirtualProtect` to mark the memory addresses that belong to the stack as an executable.
- **RopCall** (14.0.1)
Ensures that system critical APIs are called from the call instructions and not from the existing RET instructions or jump instructions.
- **RopHeap** (14.0.1)
Denies the calls to memory protection APIs to the heap that is then executed using the return instruction.
- **RopFlow**
The RopFlow technique performs a simulation of execution of return addresses in the call stack when a system critical API is called. RopFlow checks whether the RET instruction points to either another critical API or to memory that is not properly marked as executable. Either event indicates that an ROP attack occurred. RopFlow simulates a maximum allowed number of instructions to avoid a performance impact.

Memory Exploit Mitigation events are logged in to the Security log on the client and in the Memory Exploit Mitigation log on Symantec Endpoint Protection Manager. These events are similar to IPS events except that the event IDs use the signature ID range of 61000-61999.

NOTE

If you have installed or enabled the following applications on the client computers, MEM does not protect the processes that these applications protect:

Windows Enhanced Mitigation Experience Toolkit (EMET)

Microsoft Application Virtualization (App-V) feature

More information

[Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)

Preventing and handling virus and spyware attacks on client computers

You can prevent and handle virus and spyware attacks on client computers by following some important guidelines.

Table 84: Protecting computers from virus and spyware attacks

Task	Description
Make sure that your computers have Symantec Endpoint Protection installed	All computers in your network and all your servers should have Symantec Endpoint Protection installed. Make sure that Symantec Endpoint Protection is functioning correctly. See: Viewing the protection status of client computers
Keep definitions current	Make sure that the latest definitions are installed on client computers. You can check the definitions date on the Clients tab. You can run a command to update the definitions that are out of date. You can also run a computer status report to check the latest definitions date. See: How to update content and definitions on the clients

Task	Description
Run regular scans	By default, Auto-Protect and behavioral analysis (SONAR) run on client computers. A default scheduled active scan also runs on client computers. You can run scans on demand. You can customize the scan settings. See: Running on-demand scans on client computers You might want to create and customize scheduled scans. Typically, you might want to create a full scheduled scan to run once a week, and an active scan to run once per day. By default, Symantec Endpoint Protection generates an active scan that runs at 12:30 P.M. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled. You should make sure that you run an active scan every day on the computers in your network. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat in your network. Full scans consume more computer resources and might affect computer performance. See: • Setting up scheduled scans that run on Windows computers • Setting up scheduled scans that run on Mac computers • Setting up scheduled scans that run on Linux computers
Let clients upload critical events immediately	Make sure that clients (Windows only) can bypass the heartbeat interval and send critical events to the management server immediately. Critical events include any risk found (except cookies) and any intrusion event. You can find this option in Clients > Policies > Communications Settings. The option is enabled by default. Administrator notifications can alert you right away when the damper period for relevant notifications is set to None. See: Setting up administrator notifications
Check or modify scan settings for increased protection	By default, virus and spyware scans detect, remove, and repair the side effects of viruses and security risks. The default scan settings optimize your client computers' performance while still providing a high level of protection. You can increase the level of protection, however. For example, you might want to increase the Bloodhound heuristic protection. You also might want to enable scans of network drives. See: Adjusting scans to increase protection on your client computers
Allow clients to submit information about detections to Symantec	Clients can submit information about detections to Symantec. The submitted information helps Symantec address threats. See: Understanding server data collection and client submissions and their importance to the security of your network
Run intrusion prevention	Symantec recommends that you run intrusion prevention on your client computers as well as Virus and Spyware Protection. See: Managing intrusion prevention
Remediate infections if necessary	After scans run, client computers might still have infections. For example, a new threat might not have a signature, or Symantec Endpoint Protection was not able to completely remove the threat. In some cases, client computers require a restart for Symantec Endpoint Protection to complete the cleaning process. See: Removing viruses and security risks

Removing viruses and security risks

You remediate risks as part of handling virus and spyware attacks on your computers.

You use the Reports and Monitors features in the console to determine what computers are infected and to view the results of remediation.

Table 85: Removing viruses and security risks

Step	Description
Step 1: Identify infected and at-risk computers	You can get information about infected and at-risk computers from Symantec Endpoint Protection Manager. On the Home page, check the Newly Infected and the Still Infected counts in the Virus and Risks Activity Summary. The Newly Infected count is a subset of the Still Infected count. The Newly Infected count shows the number of infected and at-risk computers during the time interval that you specify in the summary. Note: Unremediated behavioral analysis (SONAR) detections are not counted as Still Infected. They are part of the Suspicious count in the summary. Computers are considered still infected if a subsequent scan detects them as infected. For example, a scheduled scan might partially clean a file. Auto-Protect subsequently detects the file as a risk. Files that are considered "still infected" are rescanned when new definitions arrive or as soon as the client computer is idle. See: Identifying the infected and at-risk computers
Step 2: Update definitions and rescan	You should make sure that clients use the latest definitions. For legacy clients that run on Windows computers, you should also make sure that your scheduled and on-demand scans use the Insight Lookup feature. Scheduled and on-demand scans always use Insight Lookup. You can check the definitions date in the Infected and At Risk Computers report. You can run the Update Content and Scan command from the Risk log. When the Virus and Risks Activity Summary on the Home page shows the Still Infected and the Newly Infected counts are zero, then all risks are eliminated. See: How to update content and definitions on the clients
Step 3: Check scan actions and rescan	Scans might be configured to leave the risk alone. You might want to edit the Virus and Spyware Protection policy and change the action for the risk category. The next time the scan runs, Symantec Endpoint Protection applies the new action. You set the action on the Actions tab for the particular scan type (administrator-defined or on-demand scan, or Auto-Protect). You can also change the detection action for Download Insight and behavioral analysis. See: Checking the scan action and rescanning the identified computers
Step 4: Restart computers if necessary to complete remediation	Computers may still be at risk or infected because they need to be restarted to finish the remediation of a virus or security risk. You can view the Risk log to determine if any computers require a restart. You can run a command from the Computer Status log to restart computers. See: Running commands on client computers from the console
Step 5: Investigate and clean remaining risks	If any risks remain, you should investigate them further. You can check the Symantec Security Response webpage for up-to-date information about viruses and security risks. See: http://securityresponse.symantec.com On the client computer, you can also access the Security Response website from the scan results dialog box. You can also run Power Eraser from Symantec Endpoint Protection Manager to analyze and remediate difficult, persistent threats. Power Eraser is an aggressive analysis that you should run on one computer or a small number of computers only when the computers are unstable or heavily infected. See: What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console Symantec Technical Support also offers a Threat Expert tool that quickly provides detailed analysis of threats. You can also run a load point analysis tool that can help you troubleshoot problems. You run these tools directly on the client computer. See: Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)

Step	Description
Step 6: Check the Computer Status log	View the Computer Status log to make sure that risks are remediated or removed from client computers. See: Viewing logs

More information

- [Virus removal and troubleshooting on a network](#)
- [Preventing and handling virus and spyware attacks on client computers](#)
- [Monitoring the Symantec Endpoint Protection clients](#)

Identifying the infected and at-risk computers

You can use the Symantec Endpoint Protection Manager Home page and a Risk report to identify the computers that are infected and at risk.

To identify infected and at-risk computers

1. In the console, click **Home** and view the Virus and Risks Activity Summary.

If you are a system administrator, you see counts of the number of Newly Infected and Still infected computers in your site. If you are a domain administrator, you see counts of the number of Newly Infected and Still infected computers in your domain.

Still Infected is a subset of Newly Infected, and the Still Infected count goes down as you eliminate the risks from your network. Computers are still infected if a subsequent scan would report them as infected. For example, Symantec Endpoint Protection might have been able to clean a risk only partially from a computer, so Auto-Protect still detects the risk.

2. In the console, click **Reports**.
3. In the **Report type** list box, click **Risk**.
4. In the **Select a report** list box, click **Infected and At Risk Computers**.
5. Click **Create Report** and note the lists of the infected and at-risk computers that appear.

More information

[Removing viruses and security risks](#)

Checking the scan action and rescanning the identified computers

If you have infected and at-risk computers, you should identify why the computers are still infected or at risk. Check the action that was taken for each risk on the infected and at-risk computers. It may be that the action that was configured and taken was Left Alone. If the action was Left Alone, you should either clean the risk from the computer, remove the computer from the network, or accept the risk. For Windows clients, you might want to edit the Virus and Spyware Protection policy and change the scan action. See:

[Removing viruses and security risks](#)

To identify the actions that need to be changed and rescan the identified computers

1. In the console, click **Monitors**.
2. On the **Logs** tab, select the Risk log, and then click **View Log**.

From the Risk log event column, you can see what happened and the action that was taken. From the Risk Name column, you can see the names of the risks that are still active. From the Domain Group User column you can see which group the computer is a member of.

If a client is at risk because a scan took the action **Left Alone**, you may need to change the Virus and Spyware Protection policy for the group. In the **Computer** column, you can see the names of the computers that still have active risks on them. See:

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

If your policy is configured to use push mode, it is pushed out to the clients in the group at the next heartbeat. See:

[Updating policies and content on the client using push mode or pull mode](#)

3. Click **Back**.
4. On the **Logs** tab, select the Computer Status log, and then click **View Log**.
5. If you changed an action and pushed out a new policy, select the computers that need to be rescanned with the new settings.
6. In the **Command** list box, select **Scan**, and then click **Start** to rescan the computers.

You can monitor the status of the Scan command from the **Command Status** tab.

How Windows clients receive definitions from the cloud

Symantec Endpoint Protection standard and embedded/VDI clients provide real-time protection with definitions in the cloud. Earlier versions provided some cloud protection with various features, such as Download Insight. Now, all virus and spyware features use the cloud to evaluate files. Cloud content includes the entire set of virus and spyware definitions as well as the latest information that Symantec has about files and potential threats.

NOTE

The Intelligent Threat Cloud Service is supported on Windows clients only.

Clients support cloud-enabled content

Cloud-enabled content includes a reduced-sized set of definitions that provides full protection. When the client requires new definitions, the client downloads or looks up the definitions in the cloud for better performance and speed.

Windows client: The client type (Reduced-sized definitions) must support cloud-enabled content. You can see the client type in **Help > Troubleshooting > Install Settings**.

Standard clients and embedded/VDI clients support cloud-enabled content.

All scans automatically use cloud lookups

Cloud lookups include queries to Symantec Insight for file reputation information and definition checking in the cloud.

- Scheduled and on-demand scans automatically perform cloud lookups.
- Auto-Protect also automatically performs cloud lookups. Auto-Protect now runs in user mode rather than kernel mode to reduce memory usage and provide better performance.

In addition to leveraging a smaller footprint with definitions on disk, the Intelligent Threat Cloud Service provides a 15-percent reduction in scan time.

Clients automatically send information about file reputation lookups to Symantec.

How cloud lookups work in your network

Symantec Endpoint Protection sends cloud lookups directly to the cloud.

If you want to use a proxy server, you can specify an HTTPS proxy in the client's browser Internet options. Or you can use the Symantec Endpoint Protection Manager console to specify the HTTPS proxy for clients in **Policies > External Communications**.

How Symantec Endpoint Protection Manager alerts you about cloud lookup errors

If clients try cloud lookups for 3 days without success, by default Symantec Endpoint Protection Manager sends an email notification to system administrators. You can also view the alert in **Monitors > Logs > System Logs > Client Activity**. The notification condition type is **File Reputation Detection**.

What are portal files?

Download Insight marks a file as a portal file when it examines a file that a user downloads from a supported portal. Scheduled and on-demand scans, Auto-Protect, and Download Insight evaluate the reputation of portal files using the sensitivity level that is set for Download Insight.

NOTE

Download Insight must be enabled to mark files as portal files.

Supported portals include: Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger, and Yahoo Messenger. The portal list (or Auto-Protect portal list) is part of the Virus and Spyware Protection content that LiveUpdate downloads to the management server or the client.

Scans and Download Insight always evaluate non-portal files with a default internal sensitivity level that Symantec sets. The internal default detects only the most malicious files.

Example of cloud lookups in action

An example of the way the Intelligent Threat Cloud Service protects clients:

- The client user runs Internet Explorer and tries to download a file. Download Insight uses its sensitivity level and reputation information from Symantec Insight in the cloud to determine that the file is not harmful.
- Download Insight determines that the file's reputation is acceptable, allows the file to download, and marks the file as a portal file.
- Later, Symantec gets more information about the file from its extensive global intelligence network. Symantec determines that the file might be harmful and updates the Insight reputation database. Symantec might provide a late-breaking signature for the file in its definitions in the cloud.
- If the user opens the file or runs a scan, Auto-Protect or the scan gets the latest information about the file from the cloud. Using the latest file reputation and the Download Insight sensitivity level, or using a late-breaking file signature, Auto-Protect or the scan now detects the file as potentially malicious.

Required and recommended settings

By default, Symantec Endpoint Protection uses the cloud. If you disable any of these options, you limit or disable cloud protection.

- **Auto-Protect**
Auto-Protect must be enabled. Auto-Protect is enabled by default.
- **Download Insight**
Download Insight must be enabled so that it can examine file downloads, and so that file downloads are marked as portal files for future scans. If you disable Download Insight, all file downloads are treated as non-portal. Scans detect only the most malicious non-portal files.
- **Insight lookups**
Insight lookups must be enabled. The Insight lookups option controls reputation lookups as well as cloud definition lookups. This option is enabled by default.

WARNING

If you disable Insight lookups, cloud protection is completely disabled.

- **Submissions**

Symantec recommends that you share information with Symantec. Data you share with Symantec improves the performance of detection features. Information about the potential malware that might attack your computers helps improve the security landscape and address threats faster. Symantec makes every attempt to make the data pseudonymous to prevent the transmission of personally identifiable information. See:
[Understanding submissions to Symantec that improve protection on your computer](#)

Managing scans on client computers

Some scans run by default, but you might want to change settings or set up your own scheduled scans. You can also customize scans and change how much protection they provide on your client computers.

NOTE

Starting in 14, scans access the complete definitions set in the cloud. See:

[How Windows clients receive definitions from the cloud](#)

Table 86: Modifying scans on client computers

Task	Description
Review the types of scans and default settings	Check your scan settings. You can review the defaults and determine if you want to make changes. See: • About the types of scans and real-time protection • About the default Virus and Spyware Protection policy scan settings
Create scheduled scans and run on-demand scans	You use scheduled scans and on-demand scans to supplement the protection that Auto-Protect provides. Auto-Protect provides protection when you read and write files. Scheduled scans and on-demand scans can scan any files that exist on your client computers. They can also protect memory, load points, and other important locations on your client computers. You can save your scheduled scan settings as a template. The scan templates can save you time when you configure multiple policies. You can use any scan that you save as a template as the basis for a new scan in a different policy. Note: For managed clients, Symantec Endpoint Protection provides a default scheduled scan that scans all files, folders, and locations on the client computers. For more information, see: • Setting up scheduled scans that run on Windows computers • Setting up scheduled scans that run on Mac computers • Setting up scheduled scans that run on Linux computers • Running on-demand scans on client computers
Customize scan settings for your environment	You can customize Auto-Protect settings as well as options in administrator-defined scans. You might want to change scan settings to handle false positive detections, optimize computer or scan performance, or change scan actions or notifications. For scheduled scans, you can also set options for missed scans, randomized scans, and whether to scan network drives. For more information, see: • Customizing the virus and spyware scans that run on Windows computers • Customizing the virus and spyware scans that run on Mac computers • Customizing the virus and spyware scans that run on Linux computers

Task	Description
Adjust scans to improve client computer performance	By default, Symantec Endpoint Protection provides a high level of security while it minimizes the effect on your client computers' performance. You can change some settings, however, to optimize the computer performance even more. Optimization is important in virtualized environments. Note: When you adjust settings to optimize client computer performance, you might decrease some security on your client computers. For more information, see: Adjusting scans to improve computer performance
Adjust scans to increase protection on your client computers	The default scan settings optimize your client computers' performance while still providing a high level of protection. You can increase the level of protection, however. See: Adjusting scans to increase protection on your client computers
Manage Download Insight detections	Download Insight inspects files that users try to download through web browsers, text messaging clients, and other portals. Download Insight uses reputation information from Symantec Insight to make decisions about files. See: Managing Download Insight detections
Manage behavioral analysis (SONAR)	Behavioral analysis is part of Proactive Threat Protection on your client computers. However, behavioral analysis settings are part of a Virus and Spyware Protection policy. See: Managing SONAR
Configure exceptions for scans	You can create exceptions for the files and applications that you know are safe. Symantec Endpoint Protection also excludes some files and folders automatically. For more information, see: • Managing exceptions in Symantec Endpoint Protection • About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans
Manage files in the Quarantine	You can monitor and delete the files that are quarantined on your client computers. You can also specify settings for the Quarantine. See: Managing the Quarantine for Windows clients
Allow clients to submit information about detections to Symantec	By default, clients send information about detections to Symantec. You can turn off submissions or choose which types of the information that clients submit. Symantec recommends that you always allow clients to send submissions. The information helps Symantec address threats. See: Understanding server data collection and client submissions and their importance to the security of your network
Manage the virus and spyware notifications that appear on client computers	You can decide whether or not notifications appear on client computers for virus and spyware events. See: Managing the virus and spyware notifications that appear on client computers

About the types of scans and real-time protection

Symantec Endpoint Protection includes different types of scans and real-time protection to detect different types of viruses, threats, and risks.

NOTE

Scans access the complete definitions set in the cloud. See:

[How Windows clients receive definitions from the cloud](#)

By default, Symantec Endpoint Protection runs an active scan every day at 12:30 P.M. Symantec Endpoint Protection also runs an active scan when new definitions arrive on the client computer. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled.

NOTE

When a client computer is off or in hibernation or sleep mode, the computer might miss a scheduled scan. When the computer starts up or wakes, by default the scan is retried within a specified interval. If the interval already expired, Symantec Endpoint Protection does not run the scan and waits until the next scheduled scan time. You can modify the settings for missed scheduled scans.

You should make sure that you run an active scan every day on the computers in your network. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat in your network. Full scans consume more computer resources and might affect computer performance. See:

[Managing scans on client computers](#)

Table 87: Scan types

Scan type	Description
Auto-Protect	Auto-Protect continuously inspects files and email data as they are written to or read from a computer. Auto-Protect automatically neutralizes or eliminates detected viruses and security risks. Mac clients and Linux clients support Auto-Protect for the file system only. On standard and embedded/VDI clients that are connected to the cloud, Auto-Protect automatically looks up the latest definitions in the cloud. For more information, see: Customizing Auto-Protect for Linux clients
Download Insight (Windows only)	Download Insight boosts the security of Auto-Protect scans by inspecting files when users try to download them from browsers and other portals. It uses reputation information from Symantec Insight to allow or block download attempts. Download Insight functions as part of Auto-Protect and requires Auto-Protect to be enabled. For more information, see: How Symantec Endpoint Protection uses Symantec Insight to make decisions about files

Scan type	Description
Administrator-defined scans	Administrator-defined scans detect viruses and security risks by examining all files and processes on the client computer. Administrator-defined scans can also inspect memory and load points. The following types of administrator-defined scans are available: Scheduled scans A scheduled scan runs on the client computers at designated times. Any concurrently scheduled scans run sequentially. If a computer is turned off or in hibernation or sleep mode during a scheduled scan, the scan does not run unless it is configured to retry missed scans. When the computer starts or wakes, Symantec Endpoint Protection retries the scan until the scan starts or the retry interval expires. You can schedule an active, full, or custom scan for Windows clients. You can schedule only a custom scan for Mac clients or Linux clients. You can save your scheduled scan settings as a template. You can use any scan that you save as a template as the basis for a different scan. The scan templates can save you time when you configure multiple policies. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and directories. Startup scans and triggered scans Startup scans run when the users log on to the computers. Triggered scans run when new virus definitions are downloaded to computers. Note: Startup scans and triggered scans are available only for Windows clients. On-demand scans On-demand scans are the scans that run immediately when you select the scan command in Symantec Endpoint Protection Manager. You can select the command from the Clients tab or from the logs. If the Symantec Endpoint Protection client for Windows detects a large number of viruses, spyware, or high-risk threats, an aggressive scan mode engages. The scan restarts and uses Insight lookups. The scan may log detections at a higher sensitivity level than the policy defines for the duration of this scan. For more information, see: Setting up scheduled scans that run on Windows computers Setting up scheduled scans that run on Mac computers
Behavioral analysis (SONAR) (Windows only)	Behavioral analysis offers real-time protection against zero-day attacks. Behavioral analysis can stop attacks even before traditional signature-based definitions detect a threat. Behavioral analysis uses heuristics as well as file reputation data to make decisions about applications or files. Like proactive threat scans, behavioral analysis detects keyloggers, spyware, and any other application that might be malicious or potentially malicious. See: What is Behavioral Analysis (SONAR) in Symantec Endpoint Protection?
Early launch anti-malware (ELAM) (Windows only)	Works with the Windows early launch anti-malware driver. Supported in Windows 8 or later and Windows Server 2012 or later. Early launch anti-malware provides protection for the computers in your network when they start up and before third-party drivers initialize. See: Managing early launch anti-malware (ELAM) detections

About the types of Auto-Protect

Auto-Protect scans files as well as certain types of email and email attachments.

By default, all types of Auto-Protect are enabled. If you use a server-based email scanning solution such as Symantec Mail Security, you might not need to enable Auto-Protect for email.

Mac clients and Linux clients do not support email Auto-Protect scans.

Table 88: Types of Auto-Protect

Type of Auto-Protect	Description
Auto-Protect	Continuously scans files as they are read from or written to the client computer. Auto-Protect is enabled by default for the file system. It loads at computer startup. It inspects all files for viruses and security risks, and blocks the security risks from being installed. It can optionally scan files by file extension, scan files on remote computers, and scan floppies for boot viruses. It can optionally back up files before it attempts to repair the files, and terminate processes and stop services. You can configure Auto-Protect to scan only selected file extensions. When Auto-Protect scans the selected extensions, it can also determine a file's type even if a virus changes the file's extension. For those clients that do not run email Auto-Protect, your client computers are still protected when Auto-Protect is enabled. Most email applications save attachments to a temporary folder when users launch email attachments. Auto-Protect scans the file as it is written to the temporary folder and detects any virus or security risk. Auto-Protect also detects the virus if the user tries to save an infected attachment to a local drive or network drive. Note: In 14.2 RU2 and later, you can configure File System Auto-Protect to automatically scan a USB drive that the computer user plugs in. See: Does Symantec Endpoint Protection Scan USB flash drives?
Microsoft Outlook Auto-Protect (Windows only)	Downloads incoming Microsoft Outlook email attachments and scans for viruses and security risks when the user reads the message and opens the attachment. The Outlook Auto-Protect plug-in supports Microsoft Outlook 98 through Outlook 2019 and Outlook 365 for the MAPI or Internet protocols. Outlook Auto-Protect supports 32-bit and 64-bit systems. Note: If Microsoft Outlook 2016 is installed with SEP, you may need to disable the Outlook Auto-Protect plug-in, or install a later version of Microsoft Outlook. See: Note: Outlook 2016 crashes when using the Endpoint Protection Add-in During installation, Symantec Endpoint Protection installs Microsoft Outlook Auto-Protect if you include it in the package and Microsoft Outlook is already installed on the computer. If a user downloads a large attachment over a slow connection, mail performance is affected. If you know the document is safe, you can create an exception. For more information, see: Excluding a file or a folder from scans Note: You should not install Microsoft Outlook Auto-Protect on a Microsoft Exchange Server. Instead you should install Symantec Mail Security for Microsoft Exchange.
Internet Email Auto-Protect (Windows only) (Available on client versions 14.2 and earlier).	Scans inbound Internet email body and email attachments for viruses and security risks; also performs outbound email heuristics scanning. By default, Internet Email Auto-Protect supports encrypted passwords and email over POP3 and SMTP connections. Internet Email Auto-Protect supports 32-bit or 64-bit systems. If you use POP3 or SMTP with Secure Sockets Layer (SSL), then the client detects secure connections but does not scan encrypted messages. Note: For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems. Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.
Lotus Notes Auto-Protect (Windows only) This feature is only available for client versions earlier than 14.2 RU1.	Scans incoming Lotus Notes email attachments for viruses and security risks. Lotus Notes Auto-Protect supports Lotus Notes 7.x or later. During installation, Symantec Endpoint Protection installs Lotus Notes Auto-Protect if you include it in the package and Lotus Notes is already installed on the computer.

More information

- [About the types of scans and real-time protection](#)
- [Customizing Auto-Protect for email scans on Windows computers](#)

About virus and security risks

Symantec Endpoint Protection scans for both viruses and for security risks. Viruses and security risks can arrive through email messages or instant messenger programs. Often a user unknowingly downloads a risk by accepting an End User License Agreement from a software program.

Many viruses and security risks are installed as drive-by downloads. These downloads usually occur when users visit malicious or infected Web sites, and the application's downloader installs through a legitimate vulnerability on the computer.

You can change the action that Symantec Endpoint Protection takes when it detects a virus or a security risk. For Windows clients, the security risk categories are dynamic and change over time as Symantec collects information about risks. See:

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)

You can view information about specific virus and security risks on the Symantec Security Response Web site.

Table 89: Viruses and security risks

Risk	Description
Viruses	Programs or code that attach a copy of themselves to another computer program or file when it runs. When the infected program runs, the attached virus program activates and attaches itself to other programs and files. The following types of threats are included in the virus category: • Malicious Internet bots Programs that run automated tasks over the Internet. Bots can be used to automate attacks on computers or to collect information from Web sites. • Worms Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate in memory to reduce computer performance. • Trojan horses Programs that hide themselves in something benign, such as a game or utility. • Blended threats Threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage. • Rootkits Programs that hide themselves from a computer's operating system.
Adware	Programs that deliver any advertising content.
Cookie	Messages that Web servers send to Web browsers for the purpose of identifying the computer or user.
Dialers	Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site. Typically, these numbers are dialed to accrue charges.
Hacking tools	Programs that hackers use to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.

Risk	Description
Joke programs	Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a joke program might move the recycle bin away from the mouse when the user tries to delete an item.
Misleading applications	Applications that intentionally misrepresent the security status of a computer. These applications typically masquerade as security notifications about any fake infections that must be removed.
Parental control programs	Programs that monitor or limit computer usage. The programs can run undetected and typically transmit monitoring information to another computer.
Remote access programs	Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer.
Security assessment tool	Programs that are used to gather information for unauthorized access to a computer.
Spyware	Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.
Trackware	Stand-alone or appended applications that trace a user's path on the Internet and send information to the controller or hacker's system.

About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans

When Symantec Endpoint Protection detects the presence of certain third-party applications and some Symantec products, it automatically creates exclusions for these files and folders. The client excludes these files and folders from all scans.

NOTE

The client does not exclude the system temporary folders from scans because doing so can create a significant security vulnerability on a computer.

To improve scan performance or reduce false positive detections, you can exclude files by adding a file or a folder exception to an Exceptions policy. You can also specify the file extensions or the folders that you want to include in a particular scan.

WARNING

The files or folders that you exclude from scans are not protected from viruses and security risks.

You can view the exclusions that the client automatically creates.

Look in the following locations of the Windows registry:

- On 32-bit computers: `HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions`
- On 64-bit computers (14.3 RU4 or earlier): `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions`.
- On 64-bit computers (14.3 RU5 or later): `HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions`

WARNING

Do not edit this registry directly.

Table 90: File and folder exclusions

Files	Description
Microsoft Exchange	The client software automatically creates file and folder scan exclusions for the following Microsoft Exchange Server versions: • Exchange 5.5 • Exchange 6.0 • Exchange 2000 • Exchange 2003 • Exchange 2007 • Exchange 2007 SP1 • Exchange 2010 • Exchange 2013 • Exchange 2016 • Exchange 2019 For Exchange 2007, see your user documentation for information about compatibility with antivirus software. In a few circumstances, you might need to create scan exclusions for some Exchange 2007 folders manually. For example, in a clustered environment, you might need to create some exclusions. The client software checks for changes in the location of the appropriate Microsoft Exchange files and folders at regular intervals. If you install Microsoft Exchange on a computer where the client software is already installed, the exclusions are created when the client checks for changes. The client excludes both files and folders; if a single file is moved from an excluded folder, the file remains excluded.
Microsoft Forefront	The client automatically creates file and folder exclusions for the following Microsoft Forefront products: • Forefront Server Security for Exchange • Forefront Server Security for SharePoint • Forefront Threat Management Gateway Check the Microsoft Web site for a list of recommended exclusions. For more information, see the following article: Configuring Symantec Endpoint Protection exclusions for Microsoft Forefront
Active Directory domain controller	The client automatically creates file and folder exclusions for the Active Directory domain controller database, logs, and working files. The client monitors the applications that are installed on the client computer. If the software detects Active Directory on the client computer, the software automatically creates the exclusions.
Symantec products	The client automatically creates appropriate file and folder scan exclusions for certain Symantec products when they are detected. The client creates exclusions for the following Symantec products: • Symantec Mail Security 4.0, 4.5, 4.6, 5.0, and 6.0 for Microsoft Exchange • Symantec AntiVirus/Filtering 3.0 for Microsoft Exchange • Norton AntiVirus 2.x for Microsoft Exchange • Symantec Endpoint Protection Manager default database (Microsoft SQL Server Express or embedded) and logs
Veritas products	The client automatically creates appropriate file and folder scan exclusions for certain Veritas products when they are detected: • Veritas Backup Exec • Veritas NetBackup • Veritas System Recovery Support for auto-exclusions of Veritas Netbackup ended with 8.x.

Files	Description
Selected extensions and Microsoft folders	For each type of administrator-defined scan or Auto-Protect, you can select files to include by extension. For administrator-defined scans, you can also select files to include by folder. For example, you can specify that a scheduled scan only scans certain extensions and that Auto-Protect scans all extensions. For executable files and Microsoft Office files, Auto-Protect can determine a file's type even if a virus changes the file's extension. By default, Symantec Endpoint Protection scans all extensions and folders. Any extensions or folders that you deselect are excluded from that particular scan. Symantec does not recommend that you exclude any extensions from scans. If you decide to exclude files by extension and any Microsoft folders, however, you should consider the amount of protection that your network requires. You should also consider the amount of time and resources that your client computers require to complete the scans. Note: Any file extensions that you exclude from Auto-Protect scans of the file system also excludes the extensions from Download Insight. If you are running Download Insight, you should include extensions for common programs and documents in the list of extensions that you want to scan. You should also make sure that you scan .msi files.
File and folder exceptions	You use an Exceptions policy to create exceptions for the files or the folders that you want Symantec Endpoint Protection to exclude from all virus and spyware scans. Note: By default, users on client computers can also create file and folder exceptions. For example, you might want to create file exclusions for an email application inbox. If the client detects a virus in the Inbox file during an on-demand or scheduled scan, the client quarantines the entire inbox. You can create an exception to exclude the inbox file instead. If the client detects a virus when a user opens an email message, however, the client still quarantines or deletes the message.
Trusted files	Virus and spyware scans use Insight, which lets scans skip trusted files. You can choose the level of trust for the files that you want to skip, or you can disable the option. If you disable the option, you might increase scan time. Auto-Protect can also skip the files that are accessed by trusted processes such as Windows Search.

More information

[Excluding a file or a folder from scans](#)

About the default Virus and Spyware Protection policy scan settings

Symantec Endpoint Protection Manager includes three default policies:

- Virus and Spyware Protection Balanced policy
- Virus and Spyware Protection High Security policy
The High Security policy is the most stringent of all the preconfigured policies. You should be aware that it can affect the performance of other applications.
- Virus and Spyware Protection High Performance policy
The High Performance policy provides better performance than the High Security policy, but it does not provide the same safeguards. The policy relies primarily on Auto-Protect to scan files with selected file extensions to detect threats.

The basic Virus and Spyware Protection policy provides a good balance between security and performance.

Table 91: Virus and Spyware Protection Balanced policy scan settings

Setting	Description
Auto-Protect for the file system	Enabled Download Insight malicious file sensitivity is set to level 5. The Download Insight action for unproven files is Ignore. Auto-Protect includes the following settings: - Scans all files for viruses and security risks. - Blocks the security risks from being installed. - Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. - Quarantines the files with security risks. Logs the files that cannot be quarantined. - Checks all floppies for boot viruses. Logs the boot viruses. - Notifies the computer users about viruses and security risks.
Auto-Protect for email	Enabled Other types of Auto-Protect include the following settings: - Scans all files, including the files that are inside compressed files. - Cleans the virus-infected files. Quarantines the files that cannot be cleaned. - Quarantines the files with security risks. Logs the files that cannot be quarantined. - Sends a message to the computer users about detected viruses and security risks.
Behavioral analysis (SONAR)	Enabled - High risk heuristic detections are quarantined - Logs any low risk heuristic detections - Aggressive mode is disabled Show alert upon detection is enabled - System change detection actions are set to Ignore. - Suspicious behavior detection blocks high risk threats and ignores low risk threats.
Administrator-defined scans	The scheduled scan includes the following default settings: - Performs an active scan every day at 12:30 P.M. The scan is randomized. - Scans all files and folders, including the files that are contained in compressed files. - Scans memory, common infection locations, and known virus and security risk locations. - Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. - Quarantines the files with security risks. Logs the files that cannot be quarantined. - Retries missed scans within three days. The on-demand scan provides the following protection: - Scans all files and folders, including the files that are contained in compressed files. - Scans memory and common infection locations. - Cleans the virus-infected files. Backs up the files before it repairs them. Quarantines the files that cannot be cleaned. - Quarantines the files with security risks. Logs the files that cannot be quarantined.

The default Virus and Spyware High Security policy provides high-level security, and includes many of the settings from the Virus and Spyware Protection policy. The policy provides increased scanning.

Table 92: Virus and Spyware Protection High Security policy settings

Setting	Description
Auto-Protect for the file system and email	Same as Virus and Spyware Protection Balanced policy Auto-Protect also inspects the files on the remote computers.
Behavioral analysis (SONAR)	Same as Virus and Spyware Protection Balanced policy but with the following changes: • Blocks any system change events.
Global settings	Bloodhound is set to Aggressive. Note: The Aggressive option is likely to produce more false positives. This option is only recommended for advanced users.

The default Virus and Spyware Protection High Performance policy provides high-level performance. The policy includes many of the settings from the Virus and Spyware Protection policy. The policy provides reduced security.

Table 93: Virus and Spyware Protection High Performance policy settings

Setting	Description
Auto-Protect for the file system	Same as Virus and Spyware Protection Balanced policy but with the following changes: • Download Insight malicious file sensitivity is set to level 1.
Microsoft Outlook Auto-Protect Internet Email Auto-Protect* Lotus Notes Auto-Protect* * Only available for client versions earlier than 14.2 RU1	Disabled
Behavior analysis (SONAR)	Same as Virus and Spyware Protection Balanced policy with the following changes: • Ignores any system change events. • Ignores any behavioral policy enforcement events.
Administrator-defined scans	Same as Virus and Spyware Protection Balanced policy.

How Symantec Endpoint Protection handles detections of viruses and security risks

Symantec Endpoint Protection uses default actions to handle the detection of viruses and security risks. You can change some of the defaults.

Table 94: How Symantec Endpoint Protection handles the detection of viruses and security risks

Detection	Description
Viruses	By default, the Symantec Endpoint Protection client first tries to clean a file that a virus infects. If the client software cannot clean the file, it does the following actions: • Moves the file to the Quarantine on the infected computer • Denies any access to the file • Logs the event
Security risks	By default, the client moves any files that security risks infect to the Quarantine on the infected computer. The client also tries to remove or repair the risk's side effects. If a security risk cannot be quarantined and repaired, the second default action is to log the risk. By default, the Quarantine contains a record of all actions that the client performed. You can return the client computer to the state that existed before the client tried the removal and repair.

Detections by behavioral analysis (SONAR) are considered suspicious events. You configure actions for these detections as part of the behavioral analysis configuration. See:

[Managing SONAR](#)

NOTE

Risky cookies are always deleted unless you specify that you want to log cookies instead. You can specify only one action for cookies, either **Delete** or **Leave alone (log only)**.

Operating system	Description
Windows	You can change the first and a second action for Symantec Endpoint Protection to take when it finds security risks. You can use different actions for scheduled, on-demand, or Auto-Protect scans. The list of the detection types for security risks is dynamic and changes as Symantec discovers new categories. New categories are downloaded to the console or the client computer when new definitions arrive.
Linux	The Linux client takes the following default actions: • <i>Malware</i>: Cleans and then quarantines the risk • <i>Security Risks</i>: Quarantines and then logs the risk. In 14.3 RU1 and later you cannot configure the actions for detections.
Mac	You can specify whether Symantec Endpoint Protection repairs the infected files that it finds. You can also specify whether Symantec Endpoint Protection moves the infected files that it cannot repair into the Quarantine. You can use different actions for scheduled, on-demand, or Auto-Protect scans.

For more information, see:

[Managing the Quarantine for Windows clients](#)

Setting up scheduled scans that run on Windows computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

Consider the following important points when you set up a scheduled scan for the Windows computers in your security network:

Multiple simultaneous scans run serially	If you schedule multiple scans to occur on the same computer and the scans start at the same time, the scans run serially. After one scan finishes, another scan starts. For example, you might schedule three separate scans on your computer to occur at 1:00 P.M. Each scan scans a different drive. One scan scans drive C. Another scan scans drive D. Another scan scans drive E. In this example, a better solution is to create one scheduled scan that scans drives C, D, and E.
Missed scheduled scans might not run	If your computer misses a scheduled scan for some reason, by default Symantec Endpoint Protection tries to perform the scan until it starts or until a specific time interval expires. If Symantec Endpoint Protection cannot start the missed scan within the retry interval, it does not run the scan.
Scheduled scan time might drift	Symantec Endpoint Protection might not use the scheduled time if the last run of the scan occurred at a different time because of the scan duration or missed scheduled scan settings. For example, you might configure a weekly scan to run every Sunday at midnight and a retry interval of one day. If the computer misses the scan and starts up on Monday at 6 A.M., the scan runs at 6 A.M. The next scan is performed one week from Monday at 6 A.M. rather than the next Sunday at midnight. If you did not restart your computer until Tuesday at 6 A.M., which is two days late and exceeds the retry interval, Symantec Endpoint Protection does not retry the scan. It waits until the next Sunday at midnight to try to run the scan. In either case, if you randomize the scan start time you might change the last run time of the scan.

NOTE

Windows settings include some options that are not available for clients that run on other operating systems.

You can click Help for more information about the options that are used in this procedure.

To set up scheduled scans that run on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined Scans**.
3. On the **Scans** tab, under **Scheduled Scans**, click **Add**.
4. In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**.
5. Click **OK**.
6. In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.
7. Click **Active Scan**, **Full Scan**, or **Custom Scan**.
8. If you selected **Custom**, under **Scanning**, you can specify the folders to scan.
9. Under **File types**, click **Scan all files** or **Scan only selected extensions**.

NOTE

Scheduled scans always scan container files unless you disable the **Scan files inside compressed files** option under **Advanced Scanning Options** or you create specific exceptions for the container file extensions.

10. Under **Enhance the scan by checking**, check or uncheck **Memory**, **Common infection locations**, or **Well-known virus and security risk locations**.
11. On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.
The retry setting under **Missed Scheduled Scans** changes automatically according to whether you select **Daily**, **Weekly**, or **Monthly**.

-
- Under **Missed Scheduled Scans**, you can disable the option to run a missed scan or you can change the retry interval.

You can also specify a maximum scan duration before the scan pauses. You can also randomize scan start time.

- If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
- Click **OK**.

More information

- [Managing scans on client computers](#)
- [Customizing administrator-defined scans for clients that run on Windows computers](#)
- [Excluding file extensions from virus and spyware scans on Windows clients and Linux clients](#)

Setting up scheduled scans that run on Mac computers

You configure scheduled scans as part of a Virus and Spyware Protection policy. See:

- [Managing scans on client computers](#)
- [Customizing administrator-defined scans for clients that run on Mac computers](#)

NOTE

Mac settings do not include all the options that are available for clients that run on Windows.

To set up scheduled scans that run on Mac computers

- In the console, open a Virus and Spyware Protection policy.
- Under **Mac Settings**, click **Administrator-defined Scans**.
- On the **Scans** tab, under **Scheduled Scans**, click **Add**.
- In the **Add Scheduled Scan** dialog box, click **Create a new scheduled scan**, and then click **OK**.
- In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and a description for the scan.
- Under **Scan drives and folders**, specify the items to scan.
- On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.

NOTE

Symantec does not recommend to run a scheduled scan more than once a day. Increasing the frequency of the scans or setting up multiple scheduled scans may cause performance issues.

- If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
- Click **OK**.

Setting up scheduled scans that run on Linux computers

You configure scheduled scans as part of a Virus and Spyware Protection policy.

To set up scheduled scans that run on Linux computers

-
1. In the console, open a Virus and Spyware Protection policy.
 2. Under **Linux Settings**, click **Administrator-defined Scans**.
 3. On the **Scans** tab, under **Scheduled Scans**, click **Add**.
 4. In the **Add Scheduled Scan** dialog box, click **Add Scheduled Scan**.
 5. In the **Add Scheduled Scan** dialog box, on the **Scan Details** tab, type a name and description for this scheduled scan.
 6. Under **Folder types**, click **Scan all folders** or specify the folders to scan.
 7. Under **File types**, click **Scan all files** or **Scan only selected extensions**.

As of 14.3 RU1, **Scan only selected extensions** option is not available.

NOTE

Scheduled scans always scan container files unless you disable the **Scan files inside compressed files** option or you create specific exceptions for the container file extensions.

8. Under **Additional options**, check or uncheck **Scan for security risks**.
9. On the **Schedule** tab, under **Scanning schedule**, set the frequency and the time at which the scan should run.
The retry setting under **Missed Scheduled Scans** changes automatically according to whether you select **Daily**, **Weekly**, or **Monthly**.
10. In 14.3 RU1 and later: Under **Missed Scheduled Scans**, you can disable the option to run a missed scan or you can change the retry interval.
11. If you want to save this scan as a template, check **Save a copy as a Scheduled Scan Template**.
12. Click **OK**.

More information

[Managing scans on client computers](#)

Running on-demand scans on client computers

You can run a manual, or on-demand, scan on client computers remotely from the management console. You might want to run an on-demand scan as part of your strategy to prevent and handle virus and spyware attacks on your client computers.

By default, an active scan runs automatically after you update definitions. You can configure an on-demand scan as a full scan or custom scan and then run the on-demand scan for more extensive scanning.

Settings for on-demand scans are similar to the settings for scheduled scans.

- For Windows client computers, you can run an active, full, or custom on-demand scan.
- For Mac client computers, you can run an active or full on-demand scan.
- For Linux client computers, you can run full on-demand scan.

The custom scan uses the settings that are configured for on-demand scans in the Virus and Spyware Protection policy.

NOTE

If you issue a restart command on a client computer that runs an on-demand scan, the scan stops, and the client computer restarts. The scan does not restart.

You can run an on-demand scan from the Computer Status log or from the **Clients** tab in the console.

You can cancel all scans in progress and queued for selected clients from the Computer Status log. If you confirm the command, the table refreshes and you see that the cancel command is added to the command status table.

To run on-demand scans on client computers

1. In the console, click **Clients**.
2. Under **Clients**, right-click the group or clients that you want to scan.
3. Do one of the following actions:
 - Click **Run a command on the group > Scan**.
 - Click **Run command on computers > Scan**.

Click **Update Content and Scan** to update definitions and then run the scan in one step.

4. For Windows clients, select **Active Scan**, **Full Scan**, or **Custom Scan**, and then click **OK**.

More information

- [Managing scans on client computers](#)
- [Preventing and handling virus and spyware attacks on client computers](#)
- [Running commands on client computers from the console](#)
- [What are the commands that you can run on client computers?](#)

Adjusting scans to improve computer performance

By default, virus and spyware scans minimize the effect on your client computers' resources. You can change some scan settings to optimize the performance even more. Many of the tasks that are suggested here are useful in the environments that run Symantec Endpoint Protection in guest operating systems on virtual machines (VMs).

Table 95: Adjusting scans to improve computer performance on Windows computers

Task	Description
Modify tuning and compressed files options for scheduled and on-demand scans	You can adjust the following options for scheduled and on-demand scans: • Change tuning options You can change the scan tuning to Best Application Performance. When you configure a scan with this setting, scans can start but they only run when the client computer is idle. If you configure an Active Scan to run when new definitions arrive, the scan might not run for up to 15 minutes if the user is using the computer • Change the number of levels to scan compressed files The default level is 3. You might want to change the level to 1 or 2 to reduce scan time. For more information, see: Customizing administrator-defined scans for clients that run on Windows computers
Use resumable scans	For computers in your network that have large volumes, scheduled scans can be configured as resumable scans. A scan duration option provides a specified period to run a scan. If the scan does not complete by the end of the specified duration, it resumes when the next scheduled scan period occurs. The scan resumes at the place where it stopped until the entire volume is scanned. Typically, you use the scan duration option on servers. Note: Do not use a resumable scan if you suspect that the computer is infected. You should perform a full scan that runs until it scans the entire computer. You should also not use a resumable scan if a scan can complete before the specified interval. For more information, see: Setting up scheduled scans that run on Windows computers

Task	Description
Adjust Auto-Protect settings	You can adjust some settings for Auto-Protect scans of the file system that might improve your client computers' performance. You can set the following options: • File cache Make sure that the file cache is enabled (the default is enabled). When the file cache is enabled, Auto-Protect remembers the clean files that it scanned and does not rescan them. • Network settings When Auto-Protect scans of remote computers are enabled, make sure that Only when files are executed is enabled. For more information, see: Customizing Auto-Protect for Windows clients
Allow all scans to skip trusted files	Virus and spyware scans include an option called Insight that skips trusted files. By default, Insight is enabled. You can change the level of trust for the types of files that scans skip: • Symantec and Community Trusted This level skips files that are trusted by Symantec and the Symantec Community. • Symantec Trusted This level skips only files that are trusted by Symantec. For more information, see: Modifying global scan settings for Windows clients
Randomize scheduled scans	In virtualized environments, where multiple virtual machines (VMs) are deployed, simultaneous scans create resource problems. For example, a single server might run 100 or more VMs. Simultaneous scans on those VMs drain resources on the server. You can randomize scans to limit the impact on your server. See: Randomizing scans to improve computer performance in virtualized environments on Windows clients
Use Shared Insight Cache in virtualized environments	Shared Insight Cache eliminates the need to rescan the files that Symantec Endpoint Protection has determined are clean. You can use Shared Insight Cache for scheduled and manual scans on your client computers. Shared Insight Cache is a separate application that you install on a server or in a virtual environment. See: Enabling the use of a network-based Shared Insight Cache
Disable early launch anti-malware (ELAM) detection	Symantec Endpoint Protection ELAM works with Windows ELAM to provide protection against malicious startup drivers. See: Managing early launch anti-malware (ELAM) detections

Table 96: Adjusting scans to improve computer performance on Mac computers

Task	Description
Enable idle-time scan	Applies to scheduled scans on clients that run on Mac computers. This option configures scheduled scans to run only while the computer is idle. See: Customizing administrator-defined scans for clients that run on Mac computers
Modify compressed files setting	Applies to Auto-Protect and on-demand scans. You can enable or disable the option, but you cannot specify the level of compressed files to scan. See: Customizing Auto-Protect for Mac clients

Table 97: Adjusting scans to improve computer performance on Linux computers

Task	Description
Scan by type of folder	The default is to scan all folder types. You can specify any of: Root , Home , Bin , Usr , Etc , and Opt . If you know that a folder is safe, you can uncheck it in the list.
Scan by file type	The default is to scan all files. If you know that a given extension is safe, you can remove it from the list.
Scan files inside compressed files	You can expand up to three levels to scan within compressed files. You might want to change the level to 1 or 2 to reduce scan time.
Scan for security risks	Lets you choose whether to scan for security risks. Security risks are updated through LiveUpdate. Scanning for security risks slows the scan down, but increases security. The default is to scan for security risks. To improve computer performance, uncheck this option.

More information[Managing scans on client computers](#)**Adjusting scans to increase protection on your client computers**

Symantec Endpoint Protection provides a high level of security by default. You can increase the protection even more. The settings are different for clients that run on Windows computers and clients that run on Mac and Linux computers.

NOTE

If you increase the protection on your client computers, you might affect computer performance.

Table 98: Adjusting scans to increase protection on Windows computers

Task	Description
Lock scan settings	Some settings are locked by default; you can lock additional settings so that users cannot change the protection on their computers.
Modify settings for administrator-defined scans	You should check or modify the following options: • Scan performance Set the scan tuning to Best Scan Performance. The setting, however, might affect your client computer performance. Scans run even if the computer is not idle. • Scheduled scan duration By default, scheduled scans run until the specified time interval expires and then resume when the client computer is idle. You can set the scan duration to Scan until finished. • Warning! Make sure that Insight Lookup is enabled. If you disable Insight lookups, cloud protection is completely disabled. Scheduled and on-demand scans always use the cloud to evaluate portal files. Auto-Protect also uses the cloud to evaluate portal files. For more information, see: • Customizing administrator-defined scans for clients that run on Windows computers • How Windows clients receive definitions from the cloud
Specify stronger scan detection actions	Specify Quarantine, Delete, or Terminate actions for detections. Note: Be careful when you use Delete or Terminate for security risk detections. The action might cause some legitimate applications to lose functionality. For more information, see: Changing the action that Symantec Endpoint Protection takes when it makes a detection

Task	Description
Increase the level of Bloodhound protection	Bloodhound locates and isolates the logical regions of a file to detect virus-like behavior. You can change the detection level from Automatic to Aggressive to increase the protection on your computers. The Aggressive setting, however, is likely to produce more false positives. See: Modifying global scan settings for Windows clients
Adjust Auto-Protect settings	You can change the following options: • File cache You can disable the file cache so that Auto-Protect rescans good files. • Network settings By default, files on network drives are scanned only when they are executed. For more information, see: Customizing Auto-Protect for Windows clients

Table 99: Adjusting scans to increase protection on Mac and Linux computers

Task	Description
Modify compressed file options for scans	The default is to scan 3 levels deep in compressed files. To increase protection, leave it at 3 levels, or change it to 3 if it is at a lower level. See: • Customizing administrator-defined scans for clients that run on Mac computers • Customizing administrator-defined scans for clients that run on Linux computers
Lock Auto-Protect settings	Some settings are locked by default; you can lock additional settings so that users cannot change the protection on their computers. On the Mac client and the Linux client, you can click Enable Auto-Protect , and then click the lock icon to lock the setting. See: • Customizing Auto-Protect for Mac clients • Customizing Auto-Protect for Linux clients
Specify stronger scan detection actions	Specify Quarantine or Delete (Linux only) actions for detections. As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client. Note: Be careful when you use Delete for security risk detections. The action might cause some legitimate applications to lose functionality. For more information, see: Changing the action that Symantec Endpoint Protection takes when it makes a detection

Managing Download Insight detections

Auto-Protect includes a feature that is called Download Insight, which examines the files that users try to download through Web browsers, text messaging clients, and other portals.

Supported portals include Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger, and Yahoo Messenger.

Download Insight determines that a downloaded file might be a risk based on evidence about the file's reputation. Download Insight is supported only for the clients that run on Windows computers.

NOTE

If you install Auto-Protect for email on your client computers, Auto-Protect also scans the files that users receive as email attachments.

For more information, see:

[Managing scans on client computers](#)

Table 100: Managing Download Insight detections

Task	Description
Learn how Download Insight uses reputation data to make decisions about files	Download Insight uses reputation information exclusively when it makes decisions about downloaded files. It does not use signatures or heuristics to make decisions. If Download Insight allows a file, Auto-Protect or behavioral analysis (SONAR) scans the file when the user opens or runs the file. See: How Symantec Endpoint Protection uses Symantec Insight to make decisions about files
View the Download Risk Distribution report to view Download Insight detections	You can use the Download Risk Distribution report to view the files that Download Insight detected on your client computers. You can sort the report by URL, Web domain, or application. You can also see whether a user chose to allow a detected file. Note: Risk details for a Download Insight detection show only the first portal application that attempted the download. For example, a user might use Internet Explorer to try to download a file that Download Insight detects. If the user then uses Firefox to try to download the file, the risk details show Internet Explorer as the portal. The user-allowed files that appear in the report might indicate false positive detections. You can also specify that you receive email notifications about new user-allowed downloads. See: Setting up administrator notifications Users can allow files by responding to notifications that appear for detections. Administrators receive the report as part of a weekly report that Symantec Endpoint Protection Manager generates and emails. You must have specified an email address for the administrator during installation or configured as part of the administrator properties. You can also generate the report from the Reports tab in the console. See: Running and customizing quick reports
Create exceptions for specific files or Web domains	You can create an exception for an application that your users download. You can also create an exception for a specific Web domain that you believe is trustworthy. See: • Creating an application exception • Excluding a trusted web domain from scans on Windows clients Note: If your client computers use a proxy with authentication, you must specify trusted Web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites. For information about the recommended exceptions, see the following articles: • How to test connectivity to Insight and Symantec licensing servers • Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers By default, Download Insight does not examine any files that users download from a trusted Internet or intranet site. You configure trusted sites and trusted local intranet sites on the Windows Control Panel > Internet Options > Security tab. When the Automatically trust any file downloaded from an intranet site option is enabled, Symantec Endpoint Protection allows any file that a user downloads from any sites in the lists. Symantec Endpoint Protection checks for updates to the Internet Options trusted sites list at user logon and every four hours. Note: Download Insight recognizes only explicitly configured trusted sites. Wildcards are allowed, but non-routable IP address ranges are not supported. For example, Download Insight does not recognize 10.*.* as a trusted site. Download Insight also does not support the sites that are discovered by the Internet Options > Security > Automatically detect intranet network option.
Make sure that Insight lookups are enabled	Download Insight requires reputation data from Symantec Insight to make decisions about files. If you disable Insight lookups, Download Insight runs but detects only the files with the worst reputations. Insight lookups are enabled by default. See: Customizing Download Insight settings

Task	Description
Customize Download Insight settings	You might want to customize Download Insight settings for the following reasons: • Increase or decrease the number of Download Insight detections. You can adjust the malicious file sensitivity slider to increase or decrease the number of detections. At lower sensitivity levels, Download Insight detects fewer files as malicious and more files as unproven. Fewer detections are false positive detections. At higher sensitivity levels, Download Insight detects more files as malicious and fewer files as unproven. More detections are false positive detections. • Change the action for malicious or unproven file detections. You can change how Download Insight handles malicious or unproven files. The specified action affects not only the detection but whether or not users can interact with the detection. For example, you might change the action for unproven files to Ignore. Then Download Insight always allows unproven files and does not alert the user. • Alert users about Download Insight detections. When notifications are enabled, the malicious file sensitivity setting affects the number of notifications that users receive. If you increase the sensitivity, you increase the number of user notifications because the total number of detections increases. You can turn off notifications so that users do not have a choice when Download Insight makes a detection. If you keep notifications enabled, you can set the action for unproven files to Ignore so that these detections are always allowed and users are not notified. Regardless of the notifications setting, when Download Insight detects an unproven file and the action is Prompt, the user can allow or block the file. If the user allows the file, the file runs automatically. When notifications are enabled and Download Insight quarantines a file, the user can undo the quarantine action and allow the file. Note: If users allow a quarantined file, the file does not automatically run. The user can run the file from the Temporary Internet Files folder. Typically, the folder location is one of the following: – Windows 8 and later: Drive:\Users\username\AppData\Local\Microsoft\Windows\INetCache – Windows Vista / 7: Drive:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files For more information, see: Customizing Download Insight settings
Allow clients to submit information about reputation detections to Symantec	By default, clients send information about reputation detections to Symantec. Symantec recommends that you enable submissions for reputation detections. The information helps Symantec address threats. See: Managing the pseudonymous or non-pseudonymous data that clients send to Symantec

How Symantec Endpoint Protection uses Symantec Insight to make decisions about files

Symantec collects information about files from its global community of millions of users and its Global Intelligence Network. The collected information is available to Symantec products in the cloud through Symantec Insight. Symantec Insight provides a file reputation database and the latest virus and spyware definitions.

Symantec products leverage Insight to protect client computers from new, targeted, and mutating threats. The data is sometimes referred to as being in the cloud since it does not reside on the client computer. Symantec Endpoint Protection must request or query Insight for information. The queries are called reputation lookups, cloud lookups, or Insight lookups.

Insight reputation ratings

Symantec Insight determines each file's level of risk or security rating. The rating is also known as the file's reputation.

Insight determines a file's security rating by examining the following characteristics of a file and its context:

-
- The source of the file
 - How new the file is
 - How common the file is in the community
 - Other security metrics, such as how the file might be associated with malware

Insight lookups

Scanning features in Symantec Endpoint Protection leverage Insight to make decisions about files and applications. Virus and Spyware Protection includes a feature that is called Download Insight. Download Insight requires reputation information to make detections. Behavioral analysis (SONAR) also uses reputation information to make detections.

To change the Insight lookups setting on

- On the **Clients** tab, go to **Policies > Settings > External Communications > Client Submissions**.

To change the Insight lookups setting on the Windows client

- Go to **Change Settings > Client Management > Submissions**.

On standard and embedded/VDI clients, the Insight lookups option also allows Auto-Protect and scheduled and manual scans to look up file reputation information as well as definitions in the cloud. Symantec recommends that you keep the option enabled.

WARNING

Download Insight, behavioral analysis (SONAR), and virus and spyware scans use Insight lookups for threat detection. Symantec recommends that you always allow Insight lookups. Disabling lookups disables Download Insight and impairs the functionality of SONAR heuristics (14.3 RU4 and earlier only) and virus and spyware scans.

File reputation submissions

By default, a client computer sends information about reputation detections to Symantec Security Response for analysis. The information helps to refine Insight's reputation database and the latest definitions in the cloud. The more clients that submit information the more useful the reputation database becomes.

Symantec recommends that you keep client submissions for reputation detections enabled.

How does Symantec Endpoint Protection use advanced machine learning?

Refer to the following topics for more information:

- [How does advanced machine learning work?](#)
- [How does AML work with the cloud?](#)
- [How do I configure AML?](#)
- [Troubleshooting advanced machine learning](#)

How does advanced machine learning work?

The advanced machine learning (AML) engine determines if a file is good or bad through a learning process. Symantec Security Response trains the engine to recognize malicious attributes and defines the rules that the AML engine uses to make detections. Symantec trains and tests the AML engine in a lab environment using the following process:

- LiveUpdate downloads the AML model to the client and runs for several days.
- The AML engine learns which applications the client runs and get exploited using the client's telemetry data. Each client computer is part of the global intelligence network that returns information about the model to Symantec.
- Symantec adjusts the AML model based on what Symantec learns from the clients' telemetry data.
- Symantec modifies the AML model to block the applications that exploits typically attack.

AML is part of the static data scanner (SDS) engine. The SDS engine includes the emulator, the Intelligent Threat Cloud Service (ITCS), and the CoreDef-3 definitions engine.

Symantec Endpoint Protection uses advanced machine learning in Download Insight, behavioral analysis (SONAR), and virus and spyware scans, all which use Insight lookups for threat detection.

How does AML work with the cloud?

Symantec leverages the Intelligent Threat Cloud Service (ITCS) to confirm the detection that AML makes on the client computer is correct. Sometimes AML may reverse the conviction after it checks with the ITCS. While the AML engine does not need Symantec Insight, this feedback enables Symantec to train the AML algorithms to reduce false positives and increase true positives. When the computer is online, Symantec Endpoint Protection can stop an average of 99% of threats. See:

- [How Windows clients receive definitions from the cloud](#)
- [How does the emulator in Symantec Endpoint Protection detect and clean malware?](#)

How do I configure AML?

You cannot configure advanced machine learning. LiveUpdate downloads the AML definitions by default. However, you do need to make sure that the following technologies are enabled.

Table 101: Steps to ensure that AML protects the client computers

Task	Description
Step 1: Make sure that cloud lookup availability is enabled	The queries that AML makes to Symantec Insight are called reputation lookups, cloud lookups, or Insight lookups. If Insight lookups are enabled, the AML detections for behavioral analysis (SONAR) and virus and spyware scans have fewer false positives. To verify that Insight lookups are enabled, see: How Symantec Endpoint Protection uses Symantec Insight to make decisions about files In addition, make sure that client submissions are enabled. This information helps Symantec measure and improve the effectiveness of detection technologies. See: Understanding server data collection and client submissions and their importance to the security of your network
Step 2: Make sure that Bloodhound Detections are enabled	Set the Bloodhound Detection level to either automatic or aggressive. See: Modifying global scan settings for Windows clients When the AML engine encounters certain high-risk files, the client automatically engages a more aggressive scan. When aggressive scan mode engages: • The scan restarts. • The following notification appears on the client: <pre>Running an aggressive scan that uses Insight lookups to clean your computer.</pre> In the aggressive mode, you may need to further manage the false positives.
Step 3: Make sure that LiveUpdate downloads high intensity definitions (optional)	LiveUpdate always downloads AML content. LiveUpdate downloads an aggressive set of definitions that work with the low bandwidth policy you get from the cloud. You can disable AML content from being downloaded through LiveUpdate. From LiveUpdate to Symantec Endpoint Protection Manager, see: Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager From Symantec Endpoint Protection Manager to the Windows clients, see: • Reverting to an older version of the Symantec Endpoint Protection security updates • About the types of content that LiveUpdate downloads

Task	Description
Step 4: Handle false positives	Manage the false positives using the Exceptions policy. See: Creating exceptions for Virus and Spyware scans Handling and preventing SONAR false positive detections Best Practice when Symantec Endpoint Protection is Detecting a File that is Believed to be Safe

Troubleshooting advanced machine learning

The logs and reports for advanced machine learning detections are the same as for the other SDS engines. To see a report with recent threats, run a Risk report for **New Risks Detected in the Network**.

You can run a scheduled report for AML detections. On the **Reports** page, click **Scheduled Reports > Add > Computer Status > Advanced Machine Learning (Static) Content Distribution**. The Symantec Endpoint Protection Manager domain must be enrolled in the cloud console for the report to appear.

For more information, see:

- [How to run scheduled reports](#)
- [Viewing logs](#)

How does the emulator in Symantec Endpoint Protection detect and clean malware?

Symantec Endpoint Protection uses a powerful emulator to protect against malware from custom packer attacks. For Auto-Protect and virus scans, this emulator improves scan performance and effectiveness by at least 10 percent from previous releases. This anti-evasion technique addresses packed malware obfuscation techniques and detects the malware that is hidden inside custom packers.

What are custom packers?

Many malware programs make use of “packers,” or the software programs that are used to compress and encrypt files for transport. These files are then executed in memory upon arrival on the user's computer.

While packers themselves are not malware, attackers use them to hide malware and obfuscate the code's real intention. Once the malware is unpacked, it executes and launches its malicious payload, often bypassing firewalls, gateways, and malware protection. Attackers have shifted from using commercial packers (such as UPX, PECompact, ASProtect, and Themida) to creating custom packers. The custom packers use proprietary algorithms to bypass standard detection techniques.

Many of the emerging custom packers are polymorphic. They use an anti-detection strategy whereby the code itself changes frequently, but the purpose and functionality of the malware remains the same. Custom packers also use clever ways of injecting the code into a target process and change its execution flow, frequently throwing off unpacker routines. Some of them are computationally intensive, calling special APIs that make the unpacking difficult.

Custom packers have grown increasingly sophisticated to hide the attack until it's too late.

How does the Symantec Endpoint Protection emulator protect against custom packers?

The high-speed emulator in Symantec Endpoint Protection fools malware into thinking it runs on the regular computer. Instead, the emulator unpacks and detonates the custom-packed file in a lightweight virtual sandbox on the client computer. The malware then opens up its payload in full, causing threats to reveal themselves in a contained environment. A static data scanner, which includes the antivirus engine and heuristics engine, acts on the payload. The sandbox is ephemeral and goes away after the threat is dealt with.

The emulator requires sophisticated technology that mimics operating systems, APIs, and processor instructions. It simultaneously manages the virtual memory and runs various heuristics and detection technologies to examine the

payload. It takes an average of 3.5 milliseconds for clean files and 300 milliseconds for malware, at about the same time it takes client users to click a file on their desktop. The emulator can detect threats quickly with minimal performance and productivity impact, so client users are not interrupted. In addition, the emulator uses a minimal amount of disk space, a maximum of 16 MB memory in the virtual environment.

The emulator works with other protection techniques, which include advanced machine learning, memory exploit mitigation, behavior monitoring, and reputation analysis. Sometimes multiple engines come into play, collaborating in a response to prevent, detect, and remediate attacks.

The emulator does not use the Internet. However, the engines within the static data scanner may require the Internet based on the malware that the emulator extracted out of the custom packer. See:

[How does Symantec Endpoint Protection use advanced machine learning?](#)

How do I configure the emulator?

The emulator is built into the Symantec Endpoint Protection software so you don't need to configure it. Symantec regularly adds or changes the emulator content for new threats and releases quarterly content updates to the emulator engine. By default, LiveUpdate automatically downloads this content with the virus and spyware definitions. See:

[Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

Symantec Endpoint Protection Manager does not include separate logs for the detections that the emulator makes. Instead, you can find any detections in the Risk log and Scan log. See:

[Viewing logs](#)

Managing the quarantine for Windows clients

You manage quarantine settings as an important part of your virus outbreak strategy.

When virus and spyware scans or behavioral analysis (SONAR) detects a threat, Symantec Endpoint Protection places the suspicious files in the infected computer's local quarantine. The client either repairs the file, repairs and restores it, or deletes it.

When the client detects a risk and quarantines the file, the client notifies the management server. You can enable the management server to automatically request and retrieve the quarantined file. The management server uploads and stores risk samples in the database, displays their event details, and lets you download them for further analysis. You may want to submit the file to your internal malware or security team for reverse engineering, or to another sandbox for analysis. If you think the conviction is a false positive, contact Broadcom Support to log a case.

NOTE

As of 14.3 RU2, you can no longer use the Central Quarantine Server. Instead, the client submits quarantined files to the Symantec Endpoint Protection Manager.

Uploading quarantined files to the management server

The management server does not retrieve quarantined files from the client by default. You must enable this setting.

To upload quarantined files

1. In the console, click **Admin > Domains > Edit Domain Properties**.
2. On the **General** tab, click **Upload quarantined files from the clients**, and then click **OK**.

To download files that the client quarantined and uploaded to the management server

1. In the console, click **Monitors > Logs >** and select the **Risk** log type.
2. Open the log, select the quarantined file, and in the **Action** drop-down list, click **Download file that the client quarantined**.

Configuring the quarantine settings

You can modify the following options for how the quarantine treats files on the client:

- What happens when new definitions arrive on clients:
By default, the client rescans items in the quarantine and automatically repairs and restores items silently when new definitions arrive. If you created an exception for a file or application in the quarantine, Symantec Endpoint Protection restores the file after new definitions arrive.
- Where quarantined items are stored:
By default, the quarantine stores backup, repaired, and quarantined files in a default folder. The quarantine clean-up feature automatically deletes the files in the quarantine when the files exceed a specified age or when the directory where they are stored reaches a certain size. It automatically deletes files after 30 days.
If you do not want to use the default quarantine directory (%ProgramData%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Quarantine) to store quarantined files on client computers, you can specify a different local directory. You can use path expansion by using the percent sign when you type the path. For example, you can type %COMMON_APPDATA%. Relative paths are not allowed.

To configure the quarantine settings

1. In the Virus and Spyware Protection policy, click **Windows Settings > Quarantine**.
2. On the **General** tab, configure the options under **When New Virus Definitions Arrive** and **Local Quarantine Options**.
Specify how to handle quarantined items and which local folder to store quarantined files. See:
[Quarantine: General](#)
3. Click **OK**.

Deleting files in the quarantine

The quarantine automatically deletes repaired files, backup files, and quarantined files after a specified number of days. You can configure the quarantine to delete files when the folder where the files are stored reaches a specified size or after a certain number of days.

You should periodically check the client computer's quarantine to prevent accumulating a large numbers of files. Check the quarantined files when a new virus outbreak appears on the network.

Leave files with unknown infections in the quarantine. When the client receives new definitions, it rescans the items in the quarantine and might delete or repair the file.

You can delete a quarantined file if a backup exists or if you have a copy of the file from a trustworthy source. You can delete a quarantined file directly on the infected computer, or by using the Risk log in the Symantec Endpoint Protection console.

NOTE

If Symantec Endpoint Protection detects risks in a compressed file, the compressed file is quarantined as a whole. However, the Risk log contains a separate entry for each file in the compressed file. To successfully delete all risks in a compressed file, you must select all the files in the compressed file.

To configure the client to delete files automatically

1. In the Virus and Spyware Protection policy, click **Windows Settings > Quarantine**.
2. On the **Cleanup** tab, check or uncheck the options to enable or disable them, and configure the time interval and size maximums. See:
[Quarantine: Cleanup](#)
3. Click **OK**.

To delete files from the Risk log

1. In the console, click **Monitors**.

-
2. On the **Logs** tab, from the **Log type** list box, select the **Risk** log, and then click **View Log**.
 3. Do one of the following actions:
 - Select an entry in the log that has a file that has been quarantined.
 - Select all entries for files in the compressed file.You must have all entries in the compressed file in the log view. You can use the **Limit** option under **Additional Settings** to increase the number of entries in the view.
 4. From the **Action** list box, select: **Delete from Quarantine**.
 5. Click **Start**.
 6. In the dialog box that appears, click **Delete**, and then **OK**.

Scanning the SEP client computer using custom YARA rules

In 14.3 RU4 and later, Symantec Endpoint Protection (SEP) and Symantec Endpoint Security (SES) provide a YARA scanner to detect malware.

Use this document to create your custom YARA rules. The YARA rules that you write are applied during on-demand scans, active scans, and scheduled scans.

NOTE

YARA rules do not work with Auto-Protect.

About YARA

Step 1: Build and compile custom YARA rules

To compile and deploy custom YARA rules, use the following YARA distribution: <https://github.com/VirusTotal/yara/releases/tag/v4.2.1>

- 14.3 RU4 and 14.3 RU5 require the YARA compiler 4.2.1.
- YARA rules that you compile with a different version of the compiler are not applied.
- YARA rules may use the PE, ELF, Math, Hash, and Time modules. A YARA ruleset that includes unsupported modules is not usable.

For more information, see:

- How to write custom YARA rules: [YARA Rules Guide: Learning this Malware Research Tool](#)
- YARA documentation and updates: <http://virustotal.github.io/yara/>

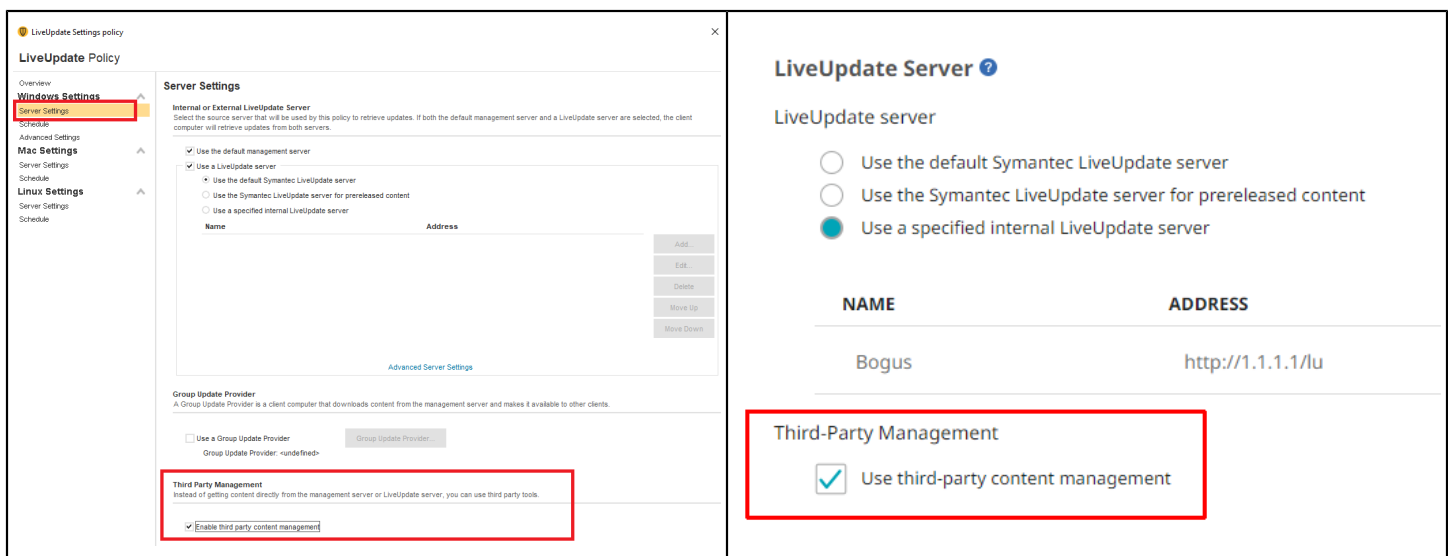
Step 2: Enable third-party management in SEP and SES

In the Symantec Endpoint Protection Manager or Symantec Endpoint Security management consoles, enable the setting to let third-party distribution tools to update managed clients.

To enable third-party management for a managed client

1. Do one of the following tasks:

SEP	SES
In the LiveUpdate policy, select Server Settings > Enable third-party content management . Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients	In the System policy, under LiveUpdate Server , select Use third-party content management LiveUpdate server settings



Step 3: Copy the compiled .yara file to the client

After you write your custom YARA rules and compile them into a .yara file, copy the .yara file to the inbox folder on the SEP client.

To copy the compiled .yara file to the client

1. Copy the .yara file to C:\ProgramData\Symantec\Symantec Endpoint Protection\Current Version\inbox.

For example: C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8262.5000\inbox

The .yara file automatically moves to the following location where the SDS definitions engine runs it: C:\ProgramData\Symantec\Symantec Endpoint Protection\14.3.8262.5000\Data\Definitions\SDSDefs

NOTE

If a folder named Invalid appears that contains your .yara file, you may not have enabled third-party management correctly in the previous step. If the .yara file disappears, you can find it in C:\ProgramData\Symantec\Symantec Endpoint Protection\Current Version\Definitions and either AdvMLDefs or SDSDefs.

Step 4: Run a scan that evaluates the custom YARA rules

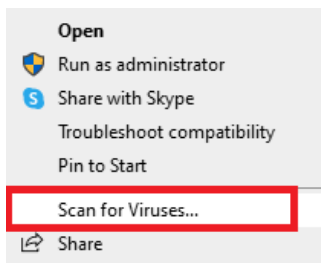
When a scan runs, the YARA rules that you supplied are used in the scan. If the scan finds a match between the rule and a pattern that is found in a malware sample, the client logs an event that specifies the rule name and metadata.

NOTE

The client logs an event only, and takes no other action.

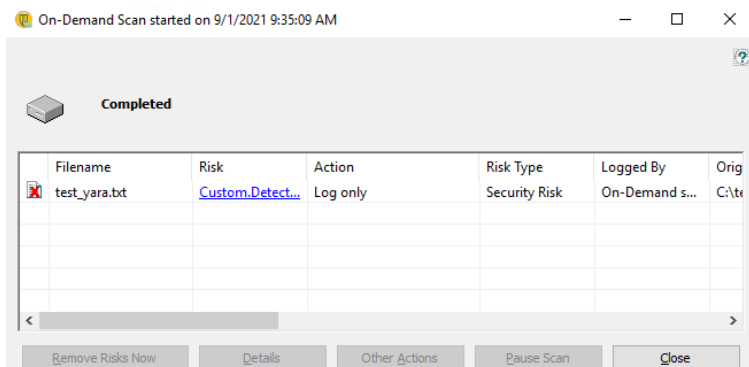
To run an on-demand scan that evaluates the custom YARA rules

1. Download the malware test files that you want to use to test the custom rule functionality to the client computer.
2. Right-click the test files and select **Scan for Viruses.....**



The results of the on-demand scan appear. Files that are detected and convicted with YARA rules are labeled as a Custom.Detection risk.

For example:



Step 5: View logs on YARA rule detections

After the scan is finished, the client uploads the information about the detection to the management console. You can view more information about the specific detection event.

To view logs on YARA rule detections

1. Do one of the following tasks:

SEP	ES																
On the Monitors page > Logs tab, select the Risk log type, and select View Log .	On the Devices page, select the device and open the Activity History tab.																
The screenshot shows the Symantec Endpoint Protection Manager interface. The 'Risk Logs' tab is selected, showing a list of events. A detailed event information window is open for a 'Custom.Detection On-Demand Scan' event. The event details include: Risk Name: Custom.Detection Source: On-Demand Scan Rule name: FirstRule Date found: 06/30/2022 13:18:10 Description: Rule name: FirstRule Actual action: Left alone Specified primary action: Leave alone (log only) Specified secondary action: Leave alone (log only) Detection source: On-Demand Scan Risk detection method: Signature-based Detection URL tracking: On Source computer: Security risk found Event type: Security risk found Database insert date: 06/30/2022 13:19:35 Event end date: 06/30/2022 13:18:10 Event client date: 06/30/2022 13:18:10	The screenshot shows the Symantec Endpoint Protection Manager interface. The 'Activity History' tab is selected for a device. The table shows the following events: <table border="1"> <thead> <tr> <th>TIME</th> <th>DESCRIPTION</th> <th>DEVICE NAME</th> <th>EVENT TYPE ID</th> </tr> </thead> <tbody> <tr> <td>Jan 13, 2022, 5:28:41 PM</td> <td>Custom Scan completed</td> <td>WIN10</td> <td>R200 Scan</td> </tr> <tr> <td>Jan 13, 2022, 5:28:41 PM</td> <td>Threat Custom.Detection</td> <td>WIN10</td> <td>R201 File Detection</td> </tr> <tr> <td>Jan 13, 2022, 5:28:41 PM</td> <td>Custom Scan started</td> <td>WIN10</td> <td>R200 Scan</td> </tr> </tbody> </table>	TIME	DESCRIPTION	DEVICE NAME	EVENT TYPE ID	Jan 13, 2022, 5:28:41 PM	Custom Scan completed	WIN10	R200 Scan	Jan 13, 2022, 5:28:41 PM	Threat Custom.Detection	WIN10	R201 File Detection	Jan 13, 2022, 5:28:41 PM	Custom Scan started	WIN10	R200 Scan
TIME	DESCRIPTION	DEVICE NAME	EVENT TYPE ID														
Jan 13, 2022, 5:28:41 PM	Custom Scan completed	WIN10	R200 Scan														
Jan 13, 2022, 5:28:41 PM	Threat Custom.Detection	WIN10	R201 File Detection														
Jan 13, 2022, 5:28:41 PM	Custom Scan started	WIN10	R200 Scan														

Replace a deployed YARA ruleset (optional)

To remove or replace a deployed YARA ruleset, deploy a new ruleset. You can also create a “dummy” ruleset which never returns a conviction. For example:

```
rule empty
{
    condition:
        false
}
```

Known issues

- The largest file size that is allowed for a compiled ruleset is 4 MB.
- A YARA ruleset that includes imports from unsupported modules fails to load properly.
- Additional YARA rules increase scan times. Symantec has built-in protection to allow only a single file to be scanned with the Yara engine for 1 second. This avoids significant performance degradation due to an overly large or complex ruleset.
- If you apply a YARA ruleset and then upgrade clients from 14.3 RU4 to 14.3 RU5 in the cloud console, the YARA ruleset filename in the Antimalware policy > **Policy Name** field is lost and replaced with **Custom YARA**. To work around this issue, reapply the YARA ruleset to the upgraded 14.3 RU5 client.

Managing the virus and spyware notifications that appear on client computers

You can decide whether or not notifications appear on client computers for virus and spyware events. You can customize messages about detections. See:

[Managing scans on client computers](#)

Table 102: Tasks for managing virus and spyware notifications that appear on client computers

Task	Description
Customize a scan detection message	For Windows and Linux client computers, you can configure a detection message for the following types of scans: • All types of Auto-Protect • Scheduled scans and on-demand scans For scheduled scans, you can configure a separate message for each scan. Note: If a process continually downloads the same security risk to a client computer, Auto-Protect automatically stops sending notifications after three detections. Auto-Protect also stops logging the event. In some situations, however, Auto-Protect does not stop sending notifications and logging events. Auto-Protect continues to send notifications and log events when the action for the detection is Leave alone (log only). For Mac client computers, you can configure a detection message that applies to all scheduled scans, to on-demand scans, and to Auto-Protect detections. These notification messages appear in the macOS Notification Center. You cannot customize the messages for Mac. For more information, see: • Customizing administrator-defined scans for clients that run on Windows computers • Customizing administrator-defined scans for clients that run on Mac computers • Customizing administrator-defined scans for clients that run on Linux computers
Change settings for user notifications about Download Insight detections	Applies to Windows client computers only. You can change the notifications that users receive about Download Insight detections. See: Managing Download Insight detections

Task	Description
Change settings for user notifications about behavioral analysis (SONAR) detections	Applies to Windows client computers only. You can change the notifications that users receive about detections. See: Managing SONAR
Choose whether or not to display the Auto-Protect results dialog	Applies to Windows client computers only. Applies to Auto-Protect for the file system only. See: Customizing administrator-defined scans for clients that run on Windows computers
Set up Auto-Protect email notifications	Applies to Windows client computers only. When Auto-Protect email scans find a risk, Auto-Protect can send email notifications to alert the email sender and any other email address that you specify. You can also insert a warning into the email message. For Internet Email Auto-Protect, you can also specify that a notification appears about scan progress when Auto-Protect scans an email. Internet Email Auto-Protect is available only to client versions earlier than 14.2 RU1. See: Customizing Auto-Protect for email scans on Windows computers
Allow users to see scan progress and start or stop scans	Applies to Windows client computers only. You can configure whether or not the scan progress dialog box appears. You can configure whether or not users are allowed to pause or delay scans. When you let users view scan progress, a link to the scan progress dialog appears in the main pages of the client user interface. A link to reschedule the next scheduled scan also appears. See: Allowing users to view scan progress and interact with scans on Windows computers
Configure warnings, errors, and prompts	Applies to Windows client computers only. You can enable or disable several types of alerts that appear on client computers about Virus and Spyware Protection events. See: Modifying log handling and notification settings on Windows computers
Enable or disable pop-up notifications on the Windows 8 style user interface	Applies to clients that run on Windows 8. You can enable or disable the pop-up notifications that appear in the Windows 8 style user interface for detections and other critical events. See: Enabling or disabling Symantec Endpoint Protection pop-up notifications that appear on Windows 8 clients

Managing early launch anti-malware (ELAM) detections

Early launch anti-malware (ELAM) provides protection for the computers in your network when they start up and before third-party drivers initialize. Malicious software can load as a driver or rootkits might attack before the operating system completely loads and Symantec Endpoint Protection starts. Rootkits can sometimes hide themselves from virus and spyware scans. Early launch anti-malware detects these rootkits and bad drivers at startup.

NOTE

ELAM is supported on Microsoft Windows 8 or later, and Windows Server 2012 or later.

Symantec Endpoint Protection provides an ELAM driver that works with the Windows ELAM driver to provide the protection. The Windows ELAM driver must be enabled for the Symantec ELAM driver to have any affect.

You use the Windows Group Policy editor to view and modify the Windows ELAM settings. See your Windows documentation for more information.

Table 103: Managing ELAM detections

Task	Description
View the status of ELAM on your client computers	You can see whether Symantec Endpoint Protection ELAM is enabled in the Computer Status log. See: Viewing logs
View ELAM detections	You can view early launch anti-malware detections in the Risk log. When Symantec Endpoint Protection ELAM is configured to report detections of bad or bad critical drivers as unknown to Windows, Symantec Endpoint Protection logs the detections as Log only . By default, Windows ELAM allows unknown drivers to load.
Enable or disable ELAM	You might want to disable Symantec Endpoint Protection ELAM to help improve computer performance. See: • Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options • Adjusting scans to improve computer performance
Adjust ELAM detection settings if you get false positives	The Symantec Endpoint Protection ELAM settings provide an option to treat bad drivers and bad critical drivers as unknown. Bad critical drivers are the drivers that are identified as malware but are required for computer startup. You might want to select the override option if you get false positive detections that block an important driver. If you block an important driver, you might prevent client computers from starting up. Note: ELAM does not support a specific exception for an individual driver. The override option applies globally to ELAM detections. For more information, see: Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options
Run Power Eraser on ELAM detections that Symantec Endpoint Protection cannot remediate	In some cases, an ELAM detection requires Power Eraser. In those cases, a message appears in the log suggesting that you run Power Eraser. You can run Power Eraser from the console. Power Eraser is also part of the Symantec Help tool. You should run Power Eraser in rootkit mode. See: • Starting Power Eraser analysis from Symantec Endpoint Protection Manager • Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)

Adjusting the Symantec Endpoint Protection early launch anti-malware (ELAM) options

Symantec Endpoint Protection provides an ELAM driver that works with the Microsoft ELAM driver to provide protection for the computers in your network when they start up. The settings are supported on Microsoft Windows 8 or later and Windows Server 2012 or later.

The Symantec Endpoint Protection ELAM driver is a special type of driver that initializes first and inspects other startup drivers for malicious code. When the driver detects a startup driver, it determines whether the driver is good, bad, or unknown. The Symantec Endpoint Protection driver then passes the information to Windows to decide to allow or block the detected driver.

You cannot create exceptions for individual ELAM detections; however, you can create a global exception to log all bad drivers as unknown. By default, unknown drivers are allowed to load.

For some ELAM detections that require remediation, you might be required to run Power Eraser. Power Eraser is part of the Symantec Help tool.

NOTE

Auto-Protect scans any driver that loads.

To adjust the Symantec Endpoint Protection ELAM options

-
1. In the Symantec Endpoint Protection Manager console, on the **Policies** tab, open a Virus and Spyware Protection policy.
 2. Under **Protection Technologies**, select **Early Launch Anti-Malware Driver**.
 3. Check or uncheck **Enable Symantec early launch anti-malware**.
The Windows ELAM driver must be enabled for this option to be enabled. You use the Windows Group Policy editor or the registry editor to view and modify the Windows ELAM settings. See your Windows documentation for more information.
 4. If you want to log the detections only, under **Detection Settings**, select **Log the detection as unknown so that Windows allows the driver to load**.
 5. Click **OK**.

[Managing early launch anti-malware \(ELAM\) detections](#)

[Troubleshooting computer issues with the Symantec Diagnostic Tool \(SymDiag\)](#)

Configuring a site to use a private Insight server for reputation queries

Private Insight server settings let you direct client reputation queries to an intranet server, if you have purchased and installed Symantec Insight for Private Clouds. Symantec Insight for Private Clouds is typically installed in networks that lack Internet connectivity. The private Insight server stores a copy of Symantec Insight's reputation database. Symantec Endpoint Protection reputation queries are handled by the private Insight server rather than Symantec's Insight server.

The private server downloads the Symantec Insight data over an encrypted, secure connection. You can manually update the Insight data or use third-party tools to check for updates and download the data automatically. Your update method depends on your network and the type of server on which you run Symantec Insight for Private Clouds.

When you use a private Insight server, Symantec does not receive any queries or submissions for file reputation.

NOTE

This task does not apply to the on-premises Symantec EDR server. See:

[Configuring clients to use Symantec EDR or private servers for reputation queries and submissions](#)

To configure a site to use a private Insight server for reputation queries

1. In the console, on the **Admin** page, select **Servers**.
2. Select the site, and then under **Tasks**, select **Edit Site Properties**.
3. On the **Private Insight Server** tab, make sure that you check **Enable private Insight server**.

You must also enter the **Name**, **Server URL**, and **Port** number.

NOTE

If you change an existing Server URL to an invalid URL, clients use the previously valid URL for the private Insight server. If the Server URL has never been configured and you enter an invalid URL, clients use the default Symantec Insight server.

At the next heartbeat, your clients start to use the specified private server for reputation queries.

More information

- [How Symantec Endpoint Protection uses Symantec Insight to make decisions about files](#)
- [Configuring client groups to use private servers for reputation queries and submissions](#)

Configuring clients to use Symantec EDR or private servers for reputation queries and submissions

You can direct client reputation queries (Insight lookups) from a group to a private intranet server. The private server can be the Symantec EDR appliance or the Symantec Insight for Private Clouds server that you purchase and install separately in your network.

The following are the private server options for groups:

- **Symantec EDR**
Symantec EDR servers gather data about client detections and provide forensic analysis. When you use a Symantec EDR server, Symantec Endpoint Protection sends all reputation queries (lookups) and most types of client submissions to Symantec EDR. Symantec EDR then sends the queries or submissions to Symantec. Note that Symantec EDR receives antivirus, behavioral analysis (SONAR), and IPS submissions, but it does not receive file reputation submissions. Symantec Endpoint Protection always sends file reputation submissions directly to Symantec.
- **Symantec Insight for Private Clouds**
This option redirects the reputation queries from clients in the group to a private Insight server. The private Insight server stores a copy of Symantec's Insight reputation database. The private Insight server handles the reputation queries rather than Symantec's Insight server. When you use a private Insight server, clients continue to send submissions about detections to Symantec. Typically, you use a private Insight server in a dark network, which is a network that is disconnected from the Internet. In that case, Symantec cannot receive any client submissions.

For more information, see:

[Understanding server data collection and client submissions and their importance to the security of your network](#)

You can also copy the private server configuration to other client groups.

You can specify multiple private servers to load balance network traffic. You can also specify multiple groups of servers to manage failover.

When you choose to enable an EDR server, the EDR connection status appears in the client user interface as well as the management console logs and reports. To communicate with the EDR server, the Symantec Endpoint Protection client must at a minimum run Virus and Spyware Protection.

To configure clients to use Symantec EDR or private server

1. In the console, go to **Clients** and select the group that should use the private server list.
2. On the **Policies** tab, click **External Communications Settings**
3. On the **Private Cloud** tab, click **Enable private servers to manage my data**.
4. Depending on which type of server you use, click **Use Symantec EDR servers for Insight lookups and submissions** or **Use private Insight servers for Insight lookups**.

You should not mix server types in the priority list.

5. Click **Use Symantec servers when private servers are not available** if you want clients to use Symantec servers for reputation queries and client antivirus and behavioral analysis (SONAR) submissions.

Clients always send file reputation submissions to Symantec.

6. Under **Private Servers**, click **Add > New Server**.
7. In the **Add Private Server** dialog, select the protocol and then enter the host name for the URL.
8. Specify the port number for the server.
9. To add a priority group, click **Add > New Group**.
10. (Optional) To apply the settings to additional client groups, click **Copy settings**. Select the groups and locations, and then click **OK**.

Customizing virus and spyware scans

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on the devices in your environment. You can also customize options for Auto-Protect.

Table 104: Customizing virus and spyware scans on Windows computers

Task	Description
Customize Auto-Protect settings	You can customize Auto-Protect in many ways, including the configuration for the following settings: • The types of files that Auto-Protect scans • The actions that Auto-Protect takes when it makes a detection • The user notifications for Auto-Protect detections You can also enable the Scan Results dialog for Auto-Protect scans of the file system. See: • Customizing Auto-Protect for Windows clients • Customizing Auto-Protect for email scans on Windows computers
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. • Compressed files • Tuning options • Advanced schedule options • User notifications about detections For more information, see: Customizing administrator-defined scans for clients that run on Windows computers You can also customize scan actions.
Adjust ELAM settings	You might want to enable or disable Symantec Endpoint Protection early launch anti-malware (ELAM) detection if you think ELAM is affecting your computers' performance. Or you might want to override the default detection setting if you get many false positive ELAM detections. See: Managing early launch anti-malware (ELAM) detections
Adjust Download Insight settings	You might want to adjust the malicious file sensitivity to increase or decrease the number of detections. You can also modify actions for detections and user notifications for detections. See: Customizing Download Insight settings
Customize scan actions	You can change the action that Symantec Endpoint Protection takes when it makes a detection. See: Changing the action that Symantec Endpoint Protection takes when it makes a detection
Customize global scan settings	You might want to customize global scan settings to increase or decrease the protection on your client computers. See: • Modifying global scan settings • Global Scan Options
Customize miscellaneous options for Virus and Spyware Protection	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. See: Modifying log handling and notification settings on Windows computers

Table 105: Customizing virus and spyware scans on Mac computers

Task	Description
Customize Auto-Protect	You can customize Auto-Protect settings for the clients that run on Mac computers. See: Customizing Auto-Protect for Mac clients
Customize administrator-defined scans	You can customize common settings and notifications as well as scan priority. You can also enable a warning to alert the user when definitions are out-of-date. See: Customizing administrator-defined scans for clients that run on Mac computers
Customize global scan options	You can specify the files or folders that you want Auto-Protect, scheduled scans, and manual scans to scan. See: • Modifying global scan settings • Mac Global Scan Options

Table 106: Customizing virus and spyware scans on Linux computers

Task	Description
Customize Auto-Protect settings	You can customize Auto-Protect in many ways, including the configuration for the following settings: • The types of files that Auto-Protect scans • The actions that Auto-Protect takes when it makes a detection As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client. • The user notifications for Auto-Protect detections You can also enable or disable the Scan Results dialog for Auto-Protect scans of the file system. See: Customizing Auto-Protect for Linux clients
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. • File and folder types • Compressed files • Security risks • Scheduling options • Actions for detections As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client. • User notifications
Customize scan actions (deprecated as of 14.3 RU1)	You can change the action that Symantec Endpoint Protection takes when it makes a detection. See: Changing the action that Symantec Endpoint Protection takes when it makes a detection
Customize global scan options (available as of 14.3 RU3)	You can customize settings that apply to all virus and spyware scans that run on your Linux clients. See: • Modifying global scan settings • Linux Global Scan Options
Customize miscellaneous options for Virus and Spyware Protection (deprecated as of 14.3 RU1)	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. See: Modifying log handling settings on Linux computers

More information[Managing scans on client computers](#)

Customizing the virus and spyware scans that run on Mac computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Mac computers. You can also customize options for Auto-Protect.

Table 107: Customizing virus and spyware scans on Mac computers

Task	Description
Customize Auto-Protect	You can customize Auto-Protect settings for the clients that run on Mac computers. See: Customizing Auto-Protect for Mac clients
Customize administrator-defined scans	You can customize common settings and notifications as well as scan priority. You can also enable a warning to alert the user when definitions are out-of-date. See: Customizing administrator-defined scans for clients that run on Mac computers
Customize global scan options	You can specify the files or folders that you want Auto-Protect, scheduled scans, and manual scans to scan. See: Modifying global scan settings

Customizing the virus and spyware scans that run on Linux computers

You can customize options for administrator-defined scans (scheduled and on-demand scans) that run on Linux computers. You can also customize options for Auto-Protect.

Table 108: Customizing virus and spyware scans on Linux computers

Task	Description
Customize Auto-Protect settings	You can customize Auto-Protect in many ways, including the configuration for the following settings: • The types of files that Auto-Protect scans • The actions that Auto-Protect takes when it makes a detection As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client. • The user notifications for Auto-Protect detections You can also enable or disable the Scan Results dialog for Auto-Protect scans of the file system. See: Customizing Auto-Protect for Linux clients
Customize administrator-defined scans	You can customize the following types of options for scheduled and on-demand scans. • File and folder types • Compressed files • Security risks • Scheduling options • Actions for detections As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client. • User notifications
Customize scan actions (deprecated as of 14.3 RU1)	You can change the action that Symantec Endpoint Protection takes when it makes a detection. See: Changing the action that Symantec Endpoint Protection takes when it makes a detection
Customize global scan options (available as of 14.3 RU3)	You can customize global settings for the scans that run on your Linux clients. See: Modifying global scan settings

Task	Description
Customize miscellaneous options for Virus and Spyware Protection (deprecated as of 14.3 RU1)	You can specify the types of risk events that clients send to Symantec Endpoint Protection Manager. See: Modifying log handling settings on Linux computers

Customizing Auto-Protect for Windows clients

You might want to customize Auto-Protect settings for Windows clients.

To configure Auto-Protect for Windows clients

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, under **Protection Technology**, click **Auto-Protect**.
3. On the **Scan Details** tab, make sure that **Enable Auto-Protect** is checked.

WARNING

If you disable Auto-Protect, Download Insight cannot function even if it is enabled.

4. Under **Scanning**, under **File types**, select one of the following options:
 - **Scan all files**
This option is the default and is the most secure option.
 - **Scan only selected extensions**
You can improve scan performance by selecting this option, however, you might decrease the protection on your computer.
5. Under **Additional options**, check or uncheck **Scan for security risks**.
6. Click **Advanced Scanning and Monitoring** to change options for the actions that trigger Auto-Protect scans and how Auto-Protect handles scans of floppy disks.
7. Click **OK**.
8. Under **Network Settings**, check or uncheck **Scan files on remote computers** to enable or disable Auto-Protect scans of network files.

By default, Auto-Protect scans files on remote computers only when the files are executed.
You might want to disable network scanning to improve scan and computer performance.
9. When file scans on remote computers is enabled, click **Network Settings** to modify network scanning options.
10. In the **Network Settings** dialog box, do any of the following actions:
 - Enable or disable Auto-Protect to trust files on the remote computers that run Auto-Protect.
 - Configure network cache options for Auto-Protect scans.
11. Click **OK**.
12. On the **Actions** tab, set any of the options. See:

[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
You can also set remediation options for Auto-Protect.
13. On the **Notifications** tab, set any of the notification options. See:

[Managing the virus and spyware notifications that appear on client computers](#)

14. On the **Advanced** tab, set any of the following options:

- **Startup and shutdown**
- **Reload options**

15. Under **Additional Options**, click **File Cache** or **Risk Tracer**.

16. Configure the file cache or Risk Tracer settings, and then click **OK**.

17. If you are finished with the configuration for this policy, click **OK**.

More information

- [Customizing the virus and spyware scans that run on Windows computers](#)
- [Managing scans on client computers](#)

Customizing Auto-Protect for Mac clients

You might want to customize Auto-Protect settings for the clients that run on Mac computers.

To customize Auto-Protect for Mac clients

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Mac Settings**, under **Protection Technology**, click **Auto-Protect and SONAR**.
3. At the top of the **Scan Details** tab, click the lock icon to lock or unlock all settings.
4. Check or uncheck any of the following options:
 - **Enable Auto-Protect**
 - **Automatically repair infected files**
 - **Quarantine files that cannot be repaired**
 - **Scan compressed files**
5. Under **General Scan Details**, specify the files that Auto-Protect scans.

NOTE

To exclude files from the scan, you must select **Scan everywhere except in specified folders**, and then add an Exceptions policy to specify the files to exclude. See:

[Excluding a file or a folder from scans](#)

6. Under **Scan Mounted Disk Details**, check or uncheck any of the available options.
7. Under **Suspicious Behavior Detection**, check or uncheck **Enable Suspicious Behavior Detection**.
This option is available as of version 14.3 RU1.
8. On the **Notifications** tab, set any of the notification options, and then click **OK**.

More information

- [Customizing the virus and spyware scans that run on Mac computers](#)
- [Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
- [Managing the virus and spyware notifications that appear on client computers](#)

Customizing Auto-Protect for Linux clients

You want to customize Auto-Protect settings for the clients that run on Linux computers.

The Virus and Spyware Protection policy contains settings for Auto-Protect Protection Technologies. The differences between the Windows and Linux operating systems mean that the Auto-Protect policy setting options are not consistent for all types of clients. Some Linux Auto-Protect options were removed in SEP 14.3 RU1.

The differences between Windows policy settings and Linux settings

- The **Actions** tab is not present for Linux Auto-Protect policies. Linux clients cannot configure specific retry actions or granular behaviors on each detection type.
- Linux has options to scan removable media.
- Linux client policies do not have these options for **Advanced Scanning and Monitoring**:
 - Floppy disk settings.
 - Backing up and Trusted files initiating Auto-Protect scans.
 - Deleting and file time preservation in **Other options**.
- Linux clients have a specific option for scanning inside compressed files in **Advanced Scanning and Monitoring**.
- Windows **Advanced** tab has options for choosing when to load Auto-Protect
- Windows has **Risk Tracer** options in the **Advanced** tab.

NOTE

Changing these options can affect your security posture and system performance. You should test changes on small groups of users first.

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Linux Settings**, under **Protection Technology**, click **Auto-Protect**.
3. On the **Scan Details** tab, check or uncheck **Enable Auto-Protect**.
4. Under **Scanning**, under **File types**, click one of the following options:
 - **Scan all files**
This option is the default and is the most secure option.
 - **Scan only selected extensions**
You improve scan performance and decrease your network's protection level, by selecting this option.
5. Under **Drive types**, check or uncheck **Removable Media**.
6. Under **Additional options**, check or uncheck **Scan for security risks**.
7. Click **Advanced Scanning and Monitoring** to change options for the actions that trigger Auto-Protect scans and how Auto-Protect handles scans of compressed files.
8. Click **OK**.
9. Under **Network Settings**, check or uncheck **Scan files on remote computers** to enable or disable Auto-Protect scans of network files.

Scanning remote files increases the security posture of your network but affects responsiveness.
10. On the **Notifications** tab, set any of the notification options. See:
[Managing the virus and spyware notifications that appear on client computers](#)
11. On the **Advanced** tab, check or uncheck **Enable the cache**.

Set a cache size or accept the default.
12. Click **OK**.

More information

-
- [Customizing the virus and spyware scans that run on Linux computers](#)
 - [Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
 - [Managing the virus and spyware notifications that appear on client computers](#)

Customizing Auto-Protect for email scans on Windows computers

You can customize Auto-Protect for email scans on Windows computers.

To customize Auto-Protect for email scans on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, select one of the following options:
 - **Microsoft Outlook Auto-Protect**
 - **Internet Email Auto-Protect***
 - **Lotus Notes Auto-Protect***

* Only available for client versions earlier than 14.2 RU1.
3. On the **Scan Details** tab, check or uncheck **Enable Internet Email Auto-Protect**.
4. Under **Scanning**, under **File types**, select one of the following options:
 - **Scan all files**
This option is the default and most secure option.
 - **Scan only selected extensions**
You can improve scan performance by selecting this option, however, you might decrease the protection on your computer.
5. Check or uncheck **Scan files inside compressed files**.
6. On the **Actions** tab, set any of the options. See:
[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
7. On the **Notifications** tab, under **Notifications**, check or uncheck **Display a notification message on the infected computer**. You can also customize the message.
8. Under **Email Notifications**, check or uncheck any of the following options:
 - **Insert a warning into the email message**
 - **Send email to the sender**
 - **Send email to others**

You can customize the message text and include a warning. For Internet Email Auto-Protect you must also specify the mail server.
9. For Internet Email Auto-Protect only, on the **Advanced** tab, under **Encrypted Connections**, enable or disable encrypted POP3 or SMTP connections.
10. Under **Mass Mailing Worm Heuristics**, check or uncheck **Outbound worm heuristics**.
11. If you are finished with the configuration for this policy, click **OK**.

More information

- [Customizing the virus and spyware scans that run on Windows computers](#)
- [Managing the virus and spyware notifications that appear on client computers](#)

Customizing administrator-defined scans for clients that run on Windows computers

You might want to customize scheduled or on-demand scans for the clients that run on Windows computers. You can set options for scans of compressed files and optimize the scan for computer or scan performance.

To customize an administrator-defined scan for the clients that run on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined scans**.
3. Do one of the following actions:
 - Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.
 - Under **Administrator On-demand Scan**, click **Edit**.
4. On the **Scan Details** tab, select **Advanced Scanning Options**:
 - On the **Compressed Files** tab, you can reduce the number of levels to scan compressed files. If you reduce the number of levels, you might improve client computer performance.
 - On the **Tuning** tab, change the tuning level for the best client computer performance or the best scan performance.Click **OK** to save changes.
5. For scheduled scans only, on the **Schedule** tab, set any of the following options:
 - **Scan Duration**
You can set how long the scan runs before it pauses and waits until the client computer is idle. You can also randomize scan start time.
 - **Missed Scheduled Scans**
You can specify a retry interval for missed scans.
6. On the **Actions** tab, change any detection actions. See:
[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
7. On the **Notifications** tab, enable or disable a notification that appears on client computers when the scan makes a detection. See:
[Managing the virus and spyware notifications that appear on client computers](#)
8. Click **OK**.

More information

- [Customizing the virus and spyware scans that run on Windows computers](#)
- [Setting up scheduled scans that run on Windows computers](#)

Customizing administrator-defined scans for clients that run on Mac computers

You customize scheduled scans and on-demand scans separately. Some of the options are different.

To customize a scheduled scan that runs on Mac computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Mac Settings**, select **Administrator-Defined Scans**.
3. Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.
For a new scan, you can create a new scan manually, or create a scheduled scan from a template.
4. On the **Scan Details** tab, under **Scan drives and folders**, select the items that you want to scan.

-
5. You can also enable or disable idle-time scans. Enabling the option improves computer performance; disabling the option improves scan performance.
 6. Click **OK**.
Edit the scan details for any other scan that is included in this policy.
 7. On the **Notifications** tab, enable or disable notification messages about scan detections. The setting applies to all scheduled scans that you include in this policy.
 8. On the **Common Settings** tab, set any of the following options:
 - **Scan Options**
 - **Actions**
 - **Alerts**These options apply to all scheduled scans that you include in this policy.
 9. Click **OK**.

To customize the on-demand scans that run on Mac computers

1. On the **Virus and Spyware Protection Policy** page, under **Mac Settings**, select **Administrator-Defined Scans**.
2. Under **Administrator On-demand Scan**, click **Edit**.
3. On the **Scan Details** tab, under **Scan drives and folders**, select the items that you want to scan.
You can also specify actions for scan detections and enable or disable scans of compressed files.
4. On the **Notifications** tab, enable or disable notifications for detections.
You can also specify the message that appears on the client.
5. Click **OK**.

More information

- [Customizing the virus and spyware scans that run on Mac computers](#)
- [Setting up scheduled scans that run on Mac computers](#)
- [Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
- [Managing the virus and spyware notifications that appear on client computers](#)

Customizing administrator-defined scans for clients that run on Linux computers

You might want to customize scheduled or on-demand scans for the clients that run on Linux computers. You can set options for scans of compressed files and optimize the scan for computer or scan performance.

To customize an administrator-defined scan for the clients that run on Linux computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Linux Settings**, click **Administrator-defined scans**.
3. Do one of the following actions:
 - Under **Scheduled Scans**, select the scheduled scan that you want to customize, or create a new scheduled scan.
 - Under **Administrator On-demand Scan**, click **Edit**.
4. On the **Scan Details** tab, check **Scan all folders** or specify the particular folders you want to scan.
5. Click **Scan all files** or **Scan only selected extensions** and specify the extensions you want to scan.
As of 14.3 RU1, **Scan only selected extensions** option is not available.

-
6. On the **Scan files inside compressed files** choice, you can reduce the number of levels to scan compressed files. If you reduce the number of levels, you might improve client computer performance.
 7. Check or uncheck **Scan for security risks**.
 8. For scheduled scans only, on the **Schedule** tab, set any of the following options:
 - **Scanning schedule**
You can set how often the scan runs, on a daily, weekly, or monthly basis.
 - **Missed Scheduled Scans**
You can specify a retry interval for missed scans.
 9. On the **Actions** tab, change any detection actions. See:
[Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.
 10. On the **Notifications** tab, enable or disable a notification that appears on client computers when the scan makes a detection. See:
[Managing the virus and spyware notifications that appear on client computers](#)
 11. Click **OK**.

More information

- [Customizing the virus and spyware scans that run on Linux computers](#)
- [Setting up scheduled scans that run on Linux computers](#)
- [Changing the action that Symantec Endpoint Protection takes when it makes a detection](#)
- [Managing the virus and spyware notifications that appear on client computers](#)

Randomizing scans to improve computer performance in virtualized environments on Windows clients

You can randomize scheduled scans to improve performance on Windows client computers. Randomization is important in virtualized environments.

For example, you might schedule scans to run at 8:00 P.M. If you select a four-hour time interval, scans on client computers start at a randomized time between 8:00 P.M. and 12:00 A.M.

To randomize scans to improve computer performance in virtualized environments

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined Scans**.
3. Create a new scheduled scan or select an existing scheduled scan to edit.
4. In the **Add Scheduled Scan** or **Edit Scheduled Scan** dialog box, click the **Schedule** tab.
5. Under **Scanning Schedule**, select how often the scan should run.
6. Under **Scan Duration**, check **Scan for up to** and select the number of hours. The number of hours controls the time interval during which scans are randomized.
7. Make sure that you enable **Randomize scan start time within this period (recommended in VMs)**.
8. Click **OK**.
9. Make sure that you apply the policy to the group that includes the computers that run Virtual Machines.

More information

-
- [Adjusting scans to improve computer performance](#)
 - [Setting up scheduled scans that run on Windows computers](#)

Modifying global scan settings

You can customize settings that apply to all virus and spyware scans that run on your client computers. You might want to modify these options to increase security on your client computers.

NOTE

If you increase the protection on your client computers by modifying these options, you might affect client computer performance.

For more information, see:

- [Managing scans on client computers](#)
- [Customizing virus and spyware scans](#)

To modify global scan settings

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, **Mac Settings**, or **Linux Settings**, click **Global Scan Options**.
3. Configure the options for any of the following operating systems:

Windows	For more information, see: Global Scan Options
Mac	For more information, see: Mac Global Scan Options
Linux	(as of 14.3 RU3) For more information, see: Linux Global Scan Options

4. Click **OK**.

Modifying log handling and notification settings on Windows computers

Each Virus and Spyware Protection policy includes the options that apply to all virus and spyware scans that run on Windows client computers.

You can set the following options:

- Specify a default URL that Symantec Endpoint Protection uses when it repairs a security risk that changed a browser home page.
- Specify Risk log handling options.
- Warn users when definitions are out-of-date or missing.
- Exclude virtual images from Auto-Protect or administrator-defined scans.

To modify log handling and notification settings on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Miscellaneous**.
Specify options for **Internet Browser Protection**.
3. On the **Log Handling** tab, set options for event filtering, log retention, and log aggregation.
4. On the **Notifications** tab, configure global notifications. See:

[Customizing the virus and spyware scans that run on Windows computers](#)

-
5. Click **OK**.

More information

[Managing the virus and spyware notifications that appear on client computers](#)

Modifying log handling settings on Linux computers

Each Virus and Spyware Protection policy includes log handling settings that apply to all virus and spyware scans that run on Linux client computers.

As of 14.3 RU1, modifying log handling settings is deprecated for the Linux client.

To log handling settings Linux computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Linux Settings**, click **Miscellaneous**.
3. On the **Log Handling** tab, set options for event filtering, log retention, and log aggregation.

More information

[Viewing logs](#)

Customizing Download Insight settings

You might want to customize Download Insight settings to decrease false positive detections on client computers. You can change how sensitive Download Insight is to the file reputation data that it uses to characterize malicious files. You can also change the notifications that Download Insight displays on client computers when it makes a detection. See:

- [Customizing the virus and spyware scans that run on Windows computers](#)
- [Managing Download Insight detections](#)

To customize Download Insight settings

1. In the console, open a Virus and Spyware Protection policy and select **Download Protection**.
2. On the **Download Insight** tab, make sure that **Enable Download Insight to detect potential risks in downloaded files based on file reputation** is checked.

If Auto-Protect is disabled, Download Insight cannot function even if it is enabled.

3. Move the slider for malicious file sensitivity to the appropriate level.

If you set the level higher, Download Insight detects more files as malicious and fewer files as unproven. Higher settings, however, return more false positives.

4. Check the following options to use as additional criteria for examining unproven files:

- **Files with x or fewer users**
- **Files known by users for x or fewer days**

When unproven files meet these criteria, Download Insight detects the files as malicious.

-
5. Make sure that **Automatically trust any file downloaded from a trusted Internet or intranet site** is checked.
 6. On the **Actions** tab, under **Malicious Files**, specify a first action and a second action.
 7. Under **Unproven Files**, specify the action.
 8. On the **Notifications** tab, specify whether or not to display a message on client computers when Download Insight makes a detection.

You can also customize the text of a warning message that appears when a user allows a file that Download Insight detects.
 9. Click **OK**.

Changing the action that Symantec Endpoint Protection takes when it makes a detection

You can configure the action or actions that scans should take when they make a detection. Each scan has its own set of actions, such as Clean, Quarantine, Delete, or Leave alone (log only).

On Windows clients and Linux clients, each detection category can be configured with a first action and a second action in case the first action is not possible.

As of 14.3 RU1, configuring the actions for detections is deprecated for the Linux client.

By default, Symantec Endpoint Protection tries to clean a file that a virus infected. If Symantec Endpoint Protection cannot clean a file, it performs the following actions:

- Moves the file to the Quarantine on the infected computer and denies any access to the file.
- Logs the event.

By default, Symantec Endpoint Protection moves any files that security risks infect into the Quarantine.

If you set the action to log only, by default if users create or save infected files, Symantec Endpoint Protection deletes them.

On Windows computers, you can also configure remediation actions for administrator scans, on-demand scans, and Auto-Protect scans of the file system.

You can lock actions so that users cannot change the action on the client computers that use this policy.

WARNING

For security risks, use the Delete action with caution. In some cases, deleting security risks causes applications to lose functionality. If you configure the client to delete the files that security risks affect, it cannot restore the files.

To back up the files that security risks affect, use the Quarantine action instead.

To change the action that Symantec Endpoint Protection takes when it makes a detection on Windows clients

1. In the Virus and Spyware Protection policy, under **Windows Settings**, select the scan (any Auto-Protect scan, administrator scan, or on-demand scan).
2. On the **Actions** tab, under **Detection**, select a type of malware or security risk.

By default, each subcategory is automatically configured to use the actions that are set for the entire category.

NOTE

On Windows clients, the categories change dynamically over time as Symantec gets new information about risks.

3. To configure actions for a subcategory only, do one of the following actions:
 - Check **Override actions configured for Malware**, and then set the actions for that subcategory only.

NOTE

There might be a single subcategory under a category, depending on how Symantec currently classifies risks. For example, under **Malware**, there might be a single subcategory called Viruses.

- Check **Override actions configured for Security Risks**, and then set the actions for that subcategory only.
- 4. Under **Actions for**, select the first and second actions that the client software takes when it detects that category of virus or security risk.
For security risks, use the Delete action with caution. In some cases, deleting security risks causes applications to lose functionality.
- 5. Repeat these steps for each category for which you want to set actions (viruses and security risks).
- 6. When you finish configuring this policy, click **OK**.

To change the action that Symantec Endpoint Protection takes when it makes a detection on Linux clients

1. In the Virus and Spyware Protection policy, under **Linux Settings**, select **Global Scan Options**.
2. Use the checkbox **Logs the detection, but does not take any action on the threat**.
3. When you finish configuring this policy, click **OK**.

To change the action that Symantec Endpoint Protection takes when it makes a detection on Mac clients

1. In the Virus and Spyware Protection policy, under **Mac Settings**, select **Administrator-Defined Scans**.
2. Do one of the following actions:
 - For scheduled scans, select the **Common Settings** tab.
 - For on-demand scans, on the **Scans** tab, under **Administrator On-demand Scan**, click **Edit**.
3. Under **Actions**, check either of the following options:
 - **Automatically repair infected files**
 - **Quarantine files that cannot be repaired**
4. For on-demand scans, click **OK**.
5. When you finish configuring this policy, click **OK**.

More information

- [Checking the scan action and rescanning the identified computers](#)
- [Removing viruses and security risks](#)

Allowing users to pause or stop scans on Windows computers

You can configure whether or not to display a scan progress dialog box on Windows client computers. If you allow the dialog box to appear on client computers, users are always allowed to pause or delay an administrator-defined scan.

The scan progress dialog box displays the progress for the currently running scan.

In addition:

- When a scan runs, the message link **scan in progress** appears.
The user can click the link to display the scan progress.
- A link to reschedule the next scheduled scan also appears.

You can allow the user to perform the following scan actions:

Pause	When a user pauses a scan, the Scan Results dialog box remains open and waits for the user to either continue or abort the scan. If the computer is turned off, the paused scan does not continue.
Snooze	When a user snoozes a scheduled scan, the user has the option of snoozing the scan for one hour or three hours. The number of snoozes is configurable. When a scan snoozes, the Scan Results dialog box closes; it reappears when the snooze period ends and the scan resumes.
Stop	When a user stops a scan, the scan usually stops immediately. If a user stops a scan while the client software scans a compressed file, the scan does not stop immediately. In this case, the scan stops as soon as the compressed file has been scanned. A stopped scan does not restart.

A paused scan automatically restarts after a specified time interval elapses.

NOTE

Users can stop a Power Eraser analysis but cannot pause or snooze it.

You can click Help for more information about the options that are used in this procedure.

To allow users to pause or stop on Windows computers

1. In the console, open a Virus and Spyware Protection policy.
2. Under **Windows Settings**, click **Administrator-defined Scans**.
3. On the **Advanced** tab, under **Scan Progress Options**, click **Show scan progress** or **Show scan progress if risk detected**.
4. To automatically close the scan progress indicator after the scan completes, check **Close the scan progress window when done**.
5. Check **Allow user to stop scan**.
6. Click **Pause Options**.
7. In the **Scan Pause Options** dialog box, do any of the following actions:
 - To limit the time that a user may pause a scan, check **Limit the time the scan may be paused**, and then type a number of minutes. The range is 3 to 180.
 - To limit the number of times a user may delay (or snooze) a scan, in the **Maximum number of snooze opportunities** box, type a number between 1 and 8.
 - By default, a user can delay a scan for one hour. To change this limit to three hours, check **Allow users to snooze the scan for 3 hours**.
8. Click **OK**.

More information

[Managing scans on client computers](#)

Configuring Windows Security Center notifications to work with Symantec Endpoint Protection clients

You can configure Windows Security Center settings on your client computers.

To configure Windows Security Center to work with Symantec Endpoint Protection clients

-
1. In the console, open a Virus and Spyware Protection policy.
 2. Under **Windows Settings**, click **Miscellaneous**.
 3. On the **Miscellaneous** tab, specify options for the Windows Security Center.
For more information about these settings, see: [Miscellaneous](#)
 4. Click **OK**.

Submitting Symantec Endpoint Protection telemetry to improve your security

Refer to the following topics for more information:

- [Introduction](#)
- [Purpose](#)
- [Enabling telemetry collection](#)
- [Frequently Asked Questions about telemetry](#)
- [Performance, sizing, and deployment](#)

Introduction

Telemetry, also known as submissions or data collection, collects information to improve the security posture of your network and improve the product experience. Telemetry broadly collects the following types of information:

- System environment, including hardware and software details
- Product errors and related events
- Effectiveness of the product configuration

The collected data is sent to Symantec.

NOTE

The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user.

Purpose

Symantec uses the information to analyze and improve product experience for customers.

- Broadcom Support uses telemetry.
- Symantec uses telemetry for insights into the threat landscape and as part of the Risk Insight program.

Enabling telemetry collection

Symantec collects telemetry data from both the management server and the Symantec Endpoint Protection client.

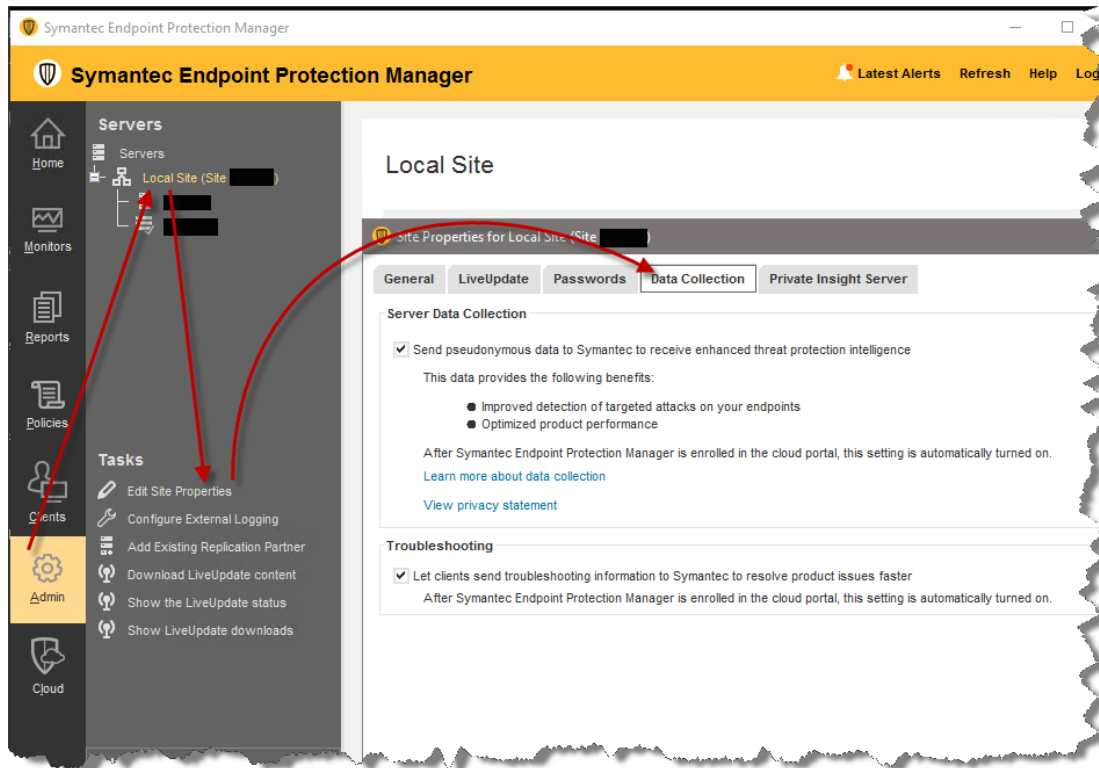
You might need to disable telemetry submissions, however, in response to network bandwidth issues or restrictions on data leaving the client. You can check the Client Activity log to view submissions activity and monitor your bandwidth usage.

To enable or disable management server telemetry collection

1. Enable or disable the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option for server data collection.
 - In the management console, go to **Admin > Servers > Local Site > Site Properties > Data Collection** and change the option.

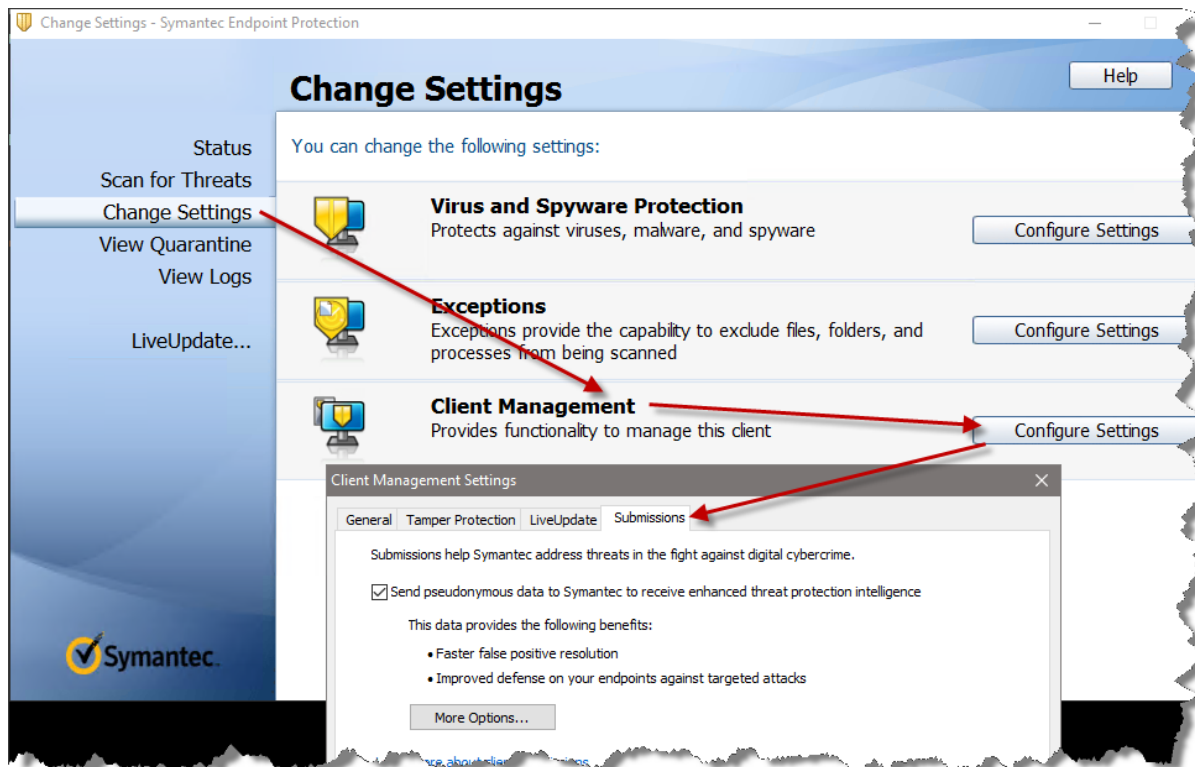
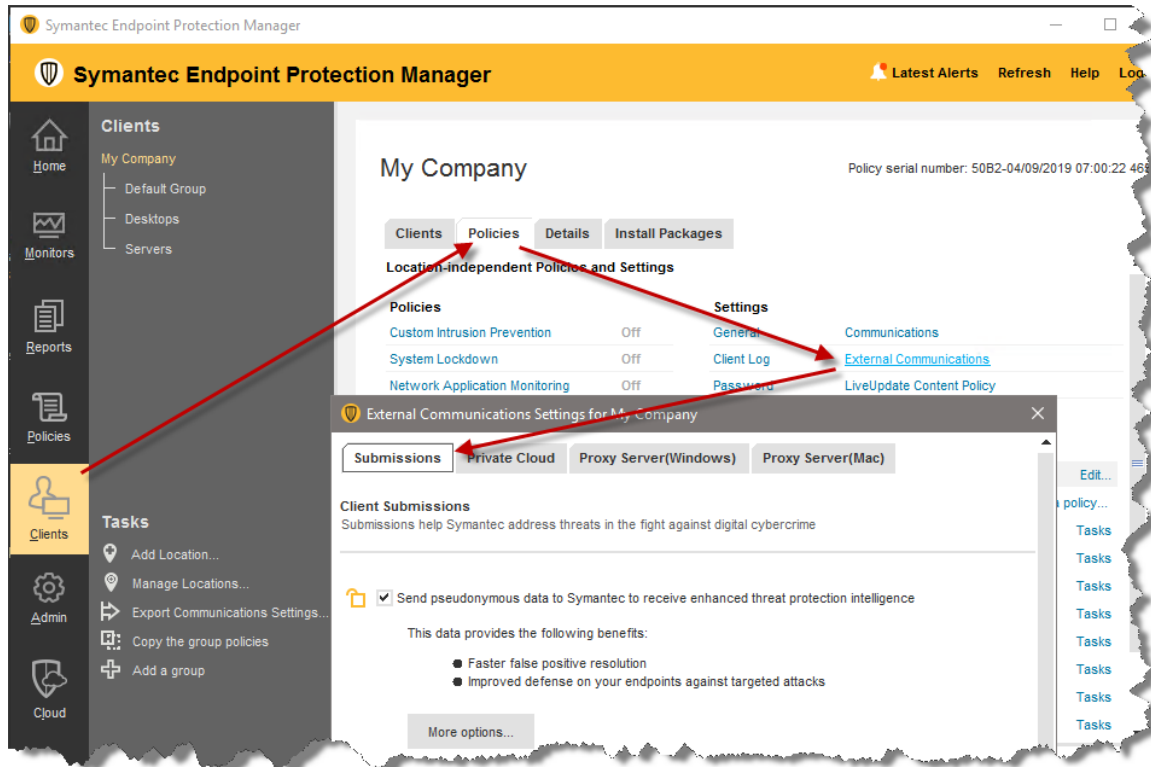
NOTE

During the installation of the Symantec Endpoint Protection Manager, you can also change the server data collection option.



To enable or disable client telemetry submissions

1. Enable or disable the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option for client submissions. You can change the option at the group level in the management console, or for a single client in the client user interface.
 - In the management console, go to **Clients > Policies** tab. In the **Settings** pane, select **External Communications Settings > Submissions**.
 - In the client user interface, go to **Change Settings > Client Management > Configure Settings > Submissions**.



Each client in the enterprise belongs to a group. A group has its own policy. In some cases, a group is configured to inherit the policy from its parent group. Since the client submissions are a group-wide setting, make sure that you apply the setting as necessary to all groups.

NOTE

If you disable submissions and lock the setting, the user cannot configure clients in the group to send submissions. If you enable the option, select submission types and lock the setting, the user cannot disable submissions. If you do not lock the setting, the user can change the configuration, including the submission types in **More Options**.

Symantec recommends that you submit threat information to help Symantec provide the best threat protection.

Frequently Asked Questions about telemetry

What types of information does Symantec Endpoint Protection collect?

For more information, see:

[Privacy and Data Protection](#)

The following table describes the type of information that Symantec Endpoint Protection collects.

Table 109: More details about the types of information that Symantec Endpoint Protection collects

Type	More Details
Software configuration, product details and installation status	Includes information about Virus and Spyware Protection policies: • Bloodhound settings Whether or not Bloodhound is enabled or disabled, and whether the level is automatic or aggressive. (Virus and Spyware Protection policy > Global Scan Options) • Download Insight settings Whether Download Insight is enabled or disabled, and what the Download Insight settings are, including the sensitivity level and prevalence threshold. (Virus and Spyware Protection policy > Download Protection) • Auto-Protect settings What overrides are configured for malware or security risks. (Virus and Spyware Protection policy > Auto-Protect) Includes information about the top 20 groups with the most number of clients. For each group, the first location, typically the default location, is selected to send the information. Typically, the information includes: • Client mode: Whether the client uses server control, client control, mixed mode, or no data found • Push/pull mode: Whether the client gets or requests policies from the server • Application learning on or off • Heartbeat interval in minutes • Upload of critical events on or off • Download randomization on or off; randomization window in minutes • Whether the client uses last-used group settings or last-used group mode • Whether the client sends detection submissions and what type, such as antivirus detections or file reputation. • Whether Host Integrity is enabled on the client • The number of domains. • The total number of groups in all domains, that is shown in approximations such as <1500. More than 3,000 is sent as >= 3000 • The maximum depth of group among all domains • The count of the total number of clients • The number of clients in computer mode • The number of clients in user mode • The number of clients in organizational unit (OU) groups
License status, license entitlement information, license ID and license usage	N/A
Device name, type, OS version, language, location, browser type and version, IP address and ID	N/A
Device hardware, software and application inventory	The server database sends the aggregate information about the client hardware. The information includes CPU, RAM, and free disk space on the Symantec Endpoint Protection installation disk.

Type	More Details
Application and database access configurations, policy requirements and policy compliance status, and application exception and workflow failure logs	Includes the number of rules for System Administrative log entries. Also sends the number of log entries as well as the number of days until the log entries expire for the following database logs: • System Administrative log • Client-Server Activity log • Audit log • System Server Activity log Includes any server replication failure events, such as replication failure or database versions that do not match.
Information associated with possible threats including: client security event information, IP address, User ID, path, device information such as device name and status, files downloaded, file actions	N/A
File and application reputation information including file downloads, actions and executing application information, and malware submissions	File reputation data is information about the files that are detected based on their reputation. • These submissions contribute to the Symantec Insight reputation database and helps protect your computers from new and emerging risks. The information includes file hash, client IP hash, IP address from where the file was downloaded, file size, and reputation score of the file.
Application exception and workflow failure logs	N/A
Personal information provided during configuration of the Service or any other subsequent service call	N/A
Licensing information such as name, version, language and licensing entitlement data	N/A
Usage of protection technologies included in SEP	Includes information about the top 20 groups with the most number of clients. For each group, the first location, typically the default location, is selected to send the information. The information includes: • The number of clients that have a particular protection technology enabled or disabled. • The number of and type (such as Quarantine, Log only, Clean, etc.) of the first and second actions for detections by the protection technologies that are enabled. Symantec Endpoint Protection Manager sends the number of shared policies of each type in its database, which is equal to the number of default policies plus the number of custom policies. The information includes: • The number of domains • The number of each of the following shared policies: – Virus and Spyware Protection policies – Firewall policies – Intrusion Prevention policies – Application and Device Control policies – LiveUpdate policies – Host Integrity policies • The number of custom intrusion prevention signatures

Type	More Details
Information that describes the configuration of SEP, such as operating system information, server hardware and software configuration specifics, CPU name, memory size, software version and features for installed packages	Includes server information such as: • Number of replication partners • Whether log data is replicated • Whether content data is replicated Includes the Linux operating system type and kernel versions, plus a count of the number of clients with this configuration. Includes the aggregation information in the Symantec Endpoint Protection Manager database about Symantec Endpoint Protection client operational state, including counts of the following: • Total clients • Reduced-size clients • Standard-size clients • EWF-enabled clients • FBWF-enabled clients • UWF-enabled clients • Microsoft hypervisor clients • VMware hypervisor clients • Citrix hypervisor clients • Unknown hypervisor clients Sends the approximate number of LiveUpdate revisions, for example <30.
Information on potential security risks, portable executable files and files with executable content that are identified as malware which may contain personal information, including information on the actions taken by such files at the time of installation	Includes the following: • Antivirus detections (Windows and Mac only) Information about virus and spyware scan detections. The type of information that clients submit includes file hash, client IP hash, antivirus signatures, attacker URL, etc. • Antivirus advanced heuristic detections (Windows only) Information about the potential threats that Bloodhound and other virus and spyware scan heuristics detect. These detections are silent and do not appear in the Risk log. Information about these detections is used for statistical analysis. • Behavioral analysis (SONAR) detections (Windows only) Information about the threats that behavioral analysis detects, which include system change events, and suspicious behavior from trusted applications. Also includes process data such as: • Behavioral analysis heuristic detections (Windows only) are silent and do not appear in the Risk log. This information is used for statistical analysis. The type of information that clients submit typically includes attributes of the detection such as the following: – Hidden processes – Small footprint processes – Keystroke logging or screen capture behavior – Disabling of security product behavior – Date and timestamps of detection

Type	More Details
Information related to network activity including URLs accessed and aggregate information on network connections (e.g., hostname, IP addresses and statistical info on a network connection)	Includes the following: • Network detection events (Windows and Mac only) Information about detections by the IPS engine (intrusion prevention). The information that clients submit includes client IP hash, attacker URL, detection timestamp, attacker IP address, IPS signature, etc. • Browser detection events (Windows only) All URLs typed in the browser address bar, clicked on, or connected to for downloading. Clients also send metadata about the following: – Each network connection, including IP addresses, port numbers, host names, applications initiating connections, protocols, connection time, number of bytes per connection. – All file transfer activities between devices, including device identification, time of the transfer, protocol, file attributes (type, name, path, size), and SHA-256 of the content.
Status information regarding installation and operation of SEP, which may contain personal information only if such information is included in the name or file folder encountered by SEP at the time of installation or error, and indicates to Symantec whether installation of SEP was successfully completed, as well as whether SEP has encountered an error	N/A
Pseudonymous general, statistical and status information	N/A

How do I know that my Symantec Endpoint Protection clients are sending telemetry submissions?

Check the Client Activity log to view submissions events. If the log does not contain current submission events, check the following:

- Make sure that client submissions are enabled.
- If you use a proxy server, check the proxy exceptions. See: [Can I specify a proxy server for client submissions?](#)
- Check connectivity to Symantec servers.
- Check to make sure that clients have current LiveUpdate content.
Symantec Endpoint Protection uses a Submission Control Data (SCD) file. Symantec publishes the SCD file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD file. The SCD file controls the following settings:
 - How many submissions a client can submit in one day
 - How long to wait before the client software retries submissions
 - How many times to retry failed submissions
 - Which IP address of the Symantec Security Response server receives the submissions

If the SCD file becomes out-of-date, then the clients stop sending submissions. Symantec considers the SCD file out-of-date when client computers have not retrieved LiveUpdate content in 7 days. The client stops sending submissions after 14 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

Can I opt out of telemetry submission?

Yes, you can opt out. You can modify the server data collection or client submissions options in the client and the server user interfaces. However, Symantec recommends that you enable as much telemetry as possible to improve the security of your network.

Performance, sizing, and deployment

How much bandwidth does telemetry consume?

Symantec Endpoint Protection throttles client computer submissions to minimize any effect on your network. Symantec Endpoint Protection throttles submissions in the following ways:

- Client computers only send samples when the computer is idle. Idle submission helps randomize the submissions traffic across the network.
- Client computers send samples for unique files only. If Symantec has already seen the file, the client computer does not send the information.

NOTE

The data size of these submissions is very negligible. For instance, antivirus submissions do not typically exceed 4 KB and similarly IPS submissions are about 32 KB in size.

Can I specify a proxy server for client submissions?

You can configure the Symantec Endpoint Protection Manager to use a proxy server for submissions and other external communications that your Windows clients use. If your client computers use a proxy with authentication, you might need to specify exceptions for Symantec URLs in your proxy server configuration. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.

For more details about the proxy, see:

[Specifying a proxy server for client submissions and other external communications](#)

To learn more about the exceptions for Symantec URLs, see:

[URLs that allow SEP and SES to connect to Symantec servers](#)

Understanding server data collection and client submissions and their importance to the security of your network

By default, Symantec Endpoint Protection clients and Symantec Endpoint Protection Manager submit some types of pseudonymous information to Symantec. Clients can also send non-pseudonymous data to Symantec to get customized analysis. You can control whether or not your clients or Symantec Endpoint Protection Manager submit information.

Both server data and client submissions are critical to improving the security of your network.

Refer to the following topics for more information:

- [What is server data collection?](#)
- [What are pseudonymous client submissions?](#)
- [What are non-pseudonymous client submissions?](#)
- [Concerns about privacy](#)
- [Concerns about bandwidth usage](#)

What is server data collection?

Server data is part of the information that helps Symantec measure and improve the efficacy of detection technologies.

Symantec Endpoint Protection Manager submits the following types of pseudonymous information to Symantec:

-
- Licensing information, which includes the name, version, language, and licensing entitlement data
 - Usage of Symantec Endpoint Protection protection features
 - Information about Symantec Endpoint Protection configuration. The information includes operating system information, server hardware and software configuration, CPU size, memory size, and software version and features for installed packages

You can change the server submissions setting during installation, or change the setting on the server's **Site Properties > Data Collection** tab in the console.

NOTE

Symantec always recommends that you keep server data collection enabled.

What are pseudonymous client submissions?

Symantec Endpoint Protection clients automatically submit pseudonymous information about detections, network, and configuration to Symantec Security Response. Symantec uses this pseudonymous information to address new and changing threats as well as to improve product performance. Pseudonymous data is not directly identified with a particular user.

The detection information that clients send includes information about antivirus detections, intrusion prevention, behavioral analysis (SONAR), and file reputation detections.

NOTE

Mac client submissions do not include behavioral analysis or file reputation submissions. Linux clients do not support any client submissions.

The pseudonymous information that clients send to Symantec benefits you by:

- Increasing the security of your network
- Optimizing product performance

In some cases, however, you might want to prevent your clients from submitting some information. For example, your corporate policies might prevent your client computers from sending any network information to outside entities. You can disable a single type of submission, such as submission of network information, rather than disabling all types of client submissions.

NOTE

Symantec recommends that you always keep client submissions enabled. Disabling submissions might interfere with faster resolution of false positive detections on the applications that are used exclusively in your organization. Without information about the malware in your organization, product response and Symantec response to threats might take longer.

For more information, see:

- [Managing the pseudonymous or non-pseudonymous data that clients send to Symantec](#)
- [How Symantec Endpoint Protection uses Symantec Insight to make decisions about files](#)

What are non-pseudonymous client submissions?

You can choose to submit non-pseudonymous client information to Symantec. This type of information provides insight into your security challenges that helps Symantec recommend customized solutions.

- You should use this option only if you participate in a Symantec-sponsored program that provides you custom analysis.
- The option is disabled by default.

For more information, see:

[Managing the pseudonymous or non-pseudonymous data that clients send to Symantec](#)

Concerns about privacy

Symantec makes every attempt to pseudonymize the client submission data.

- Only suspicious executable files are submitted.
- User names are removed from path names.
- Computers and enterprises are identified by unique pseudonymized values.
- IP addresses are used for geographic location and then discarded.

For more information about privacy, see the following document:

[Privacy statement](#)

Concerns about bandwidth usage

Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth.

You can check the Client Activity log to view the types of submissions that your client computers send and to monitor bandwidth usage. See:

- [How Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth](#)
- [Viewing logs](#)

Managing the pseudonymous or non-pseudonymous data that clients send to Symantec

Symantec Endpoint Protection can protect computers by submitting pseudonymous information about detections to Symantec. Symantec uses this information to address new and changing threats. Any data you submit improves Symantec's ability to respond to threats and customize protection for your computers. Symantec recommends that you choose to submit as much detection information as possible. See:

[Understanding server data collection and client submissions and their importance to the security of your network](#)

Client computers submit information pseudonymously about detections. You can specify the types of detections for which clients submit information. The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user.

NOTE

Mac client submissions do not include behavioral analysis (SONAR) or file reputation submissions. Linux clients do not support any client submissions.

To change client submission settings

1. In the console, select **Clients** then click the **Policies** tab.
2. In the **Settings** pane, click **External Communications Settings**.
3. Select the **Client Submissions** tab.
4. Enable or disable the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option.
5. Select **More options** if you want to enable or disable specific submission types, such as file reputation.
6. If you participate in a Symantec-sponsored custom analysis program, select **Send client-identifiable data to Symantec for custom analysis**.

WARNING

This option sends non-pseudonymous information to Symantec. Only use this option if you participate in a Symantec-sponsored program and want to share client-identifiable data with Symantec.

7. Select **OK**.

NOTE

On Mac clients, you can also disable IPS ping submissions. See the following article:

[How to disable IPS data submission on Symantec Endpoint Protection for Mac clients](#)

How Symantec Endpoint Protection minimizes the impact of client submissions on your network bandwidth

Symantec Endpoint Protection throttles client computer submissions to minimize any effect on your network. Symantec Endpoint Protection throttles submissions in the following ways:

- Client computers only send samples when the computer is idle. Idle submission helps randomize the submissions traffic across the network.
- Client computers send samples for unique files only. If Symantec has already seen the file, the client computer does not send the information.
- Symantec Endpoint Protection uses a Submission Control Data (SCD) file. Symantec publishes the SCD file and includes it as part of a LiveUpdate package. Each Symantec product has its own SCD file.

The SCD file controls the following settings:

- How many submissions a client can submit in one day
- How long to wait before the client software retries submissions
- How many times to retry failed submissions
- Which IP address of the Symantec Security Response server receives the submission

If the SCD file becomes out-of-date, then clients stop sending submissions. Symantec considers the SCD file out-of-date when a client computer has not retrieved LiveUpdate content in 7 days. The client stops sending submissions after 14 days.

If clients stop the transmission of the submissions, the client software does not collect the submission information and send it later. When clients start to transmit submissions again, they only send the information about the events that occur after the transmission restart.

More information

[Understanding server data collection and client submissions and their importance to the security of your network](#)

Specifying a proxy server for client submissions and other external communications

You can configure Symantec Endpoint Protection Manager to use a proxy server for submissions and other external communications that your Windows clients use.

NOTE

If your client computers use a proxy with authentication, you might need to specify exceptions for Symantec URLs in your proxy server configuration. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites.

You need to include exceptions for Symantec URLs in your proxy server settings if you use the following proxy configuration options:

- You use a proxy server with authentication.
- You select **Use a proxy server specified by my client browser** option in the Symantec Endpoint Protection Manager **External Communication Dialog**.
- You use auto-detection or auto-configuration in your browser's Internet Options.

You do not have to specify exceptions for Symantec URLs in your proxy server settings if you do not use auto-detection or auto-configuration. You should select **Use custom proxy settings** in the **External Communication** dialog and then specify the authentication settings.

To specify a proxy server for client submissions and other external communications

1. In the console, on the **Clients** page, select the group and then click **Policies**.
2. Under **Settings** or **Location-specific Settings**, click **External Communications**.
3. On the **Proxy Server (Windows)** tab, under **HTTPS Proxy Configuration**, select **Use custom proxy settings**.
4. Enter the information about the proxy server that your clients use. See the online Help for more information about the options.
5. Click **OK**.

For information about the recommended exceptions, see the following articles:

- [How to test connectivity to Insight and Symantec licensing servers](#)
- [Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers](#)

More information

- [Understanding server data collection and client submissions and their importance to the security of your network](#)
- [Creating exceptions for Virus and Spyware scans](#)

Managing Behavioral Analysis (SONAR)

Behavioral analysis is part of Proactive Threat Protection on your client computers and the Virus and Spyware Protection policy in Symantec Endpoint Protection Manager.

Table 110: Managing behavioral analysis

Task	Description
Learn how SONAR works	Learn how behavioral analysis detects unknown threats. This information can help you make decisions about using behavioral analysis in your security network. See: What is Behavioral Analysis (SONAR) in Symantec Endpoint Protection?
Check that SONAR is enabled	Behavioral analysis interoperates with some other Symantec Endpoint Protection features. Behavioral analysis requires Auto-Protect. You can use the Clients tab to check whether Proactive Threat Protection is enabled on your client computers. See: Adjusting SONAR settings on your client computers
Check the default settings for behavioral analysis	Behavioral analysis settings are part of a Virus and Spyware Protection policy. See: About the default Virus and Spyware Protection policy scan settings

Task	Description
Make sure that Insight lookups are enabled	Behavioral analysis uses reputation data in addition to heuristics to make detections. If you disable Insight lookups, behavioral analysis makes detections by using heuristics only. The rate of false positives might increase, and the protection that SONAR provides is limited. You enable or disable Insight Lookups in the Submissions dialog. See: Understanding server data collection and client submissions and their importance to the security of your network
Monitor behavioral analysis events to check for false positive detections	You can use the behavioral analysis log to monitor events. You can also view the SONAR Detection Results report (under Risk Reports) to view information about detections. See: • Monitoring SONAR detection results to check for false positives • Monitoring the Symantec Endpoint Protection clients
Adjust behavioral analysis settings	You can change the detection action for some types of threats that behavioral analysis detects. You might want to change the detection action to reduce false positive detections. You also might want to enable or disable notifications for high or low risk heuristic detections. See: • Adjusting SONAR settings on your client computers • Handling and preventing SONAR false positive detections
Prevent behavioral analysis from detecting the applications that you know are safe	SONAR might detect the files or applications that you want to run on your client computers. You can use an Exceptions policy to specify exceptions for the specific files, folders, or applications that you want to allow. For the items that SONAR quarantines, you can create an exception for the quarantined item from the SONAR log. You also might want to set SONAR actions to log and allow detections. You can use application learning so that Symantec Endpoint Protection learns the legitimate applications on your client computers. In 14.3 RU4 and earlier, after Symantec Endpoint Protection learns the applications that you use in your network, you can change the SONAR action to Quarantine. Note: If you set the action for high risk detections to log only, you might allow potential threats on your client computers. For more information, see: Handling and preventing SONAR false positive detections
Prevent behavioral analysis from examining some applications	In some cases, an application might become unstable or cannot run when behavioral analysis injects code into the application to examine it. You can create a file, folder, or application exception for the application. See: Creating exceptions for Virus and Spyware scans
Manage the way behavioral analysis detects the applications that make DNS or host file changes	You can globally adjust the way SONAR handles detections of DNS or host file changes. You can use the Exceptions policy to configure exceptions for specific applications. See: • Adjusting SONAR settings on your client computers • Creating an exception for an application that makes a DNS or host file change
Allow clients to submit information about behavioral analysis detections to Symantec	Symantec recommends that you enable submissions on your client computers. The information that clients submit about detections helps Symantec address threats. The information helps Symantec create better heuristics, which results in fewer false positive detections. See: Understanding server data collection and client submissions and their importance to the security of your network

What is Behavioral Analysis (SONAR) in Symantec Endpoint Protection?

Behavioral analysis is the real-time protection that detects potentially malicious behavior when applications run on your computers. Behavioral analysis uses heuristics as well as reputation data to detect emerging and unknown threats. Behavioral analysis provides "zero-day" protection because it detects malicious behavior before traditional virus and spyware detection definitions have been created to address the threats.

Behavioral analysis provides an additional level of protection on your client computers and complements your existing Virus and Spyware Protection, intrusion prevention, Memory Exploit Mitigation, and firewall protection.

Behavioral analysis uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on your client computers to detect emerging threats. Behavioral analysis also detects changes or behavior on your client computers that you should monitor.

NOTE

Auto-Protect also uses a type of heuristic that is called Bloodhound to detect suspicious behavior in files.

Behavioral analysis might inject some code into the applications that run in Windows user mode to monitor them for suspicious activity. In some cases, the injection might affect the application performance or cause problems with running the application. You can create an exception to exclude the file, folder, or application from this type of monitoring.

Behavioral analysis does not make detections on application type, but on how a process behaves. Behavioral analysis acts on an application only if that application behaves maliciously, regardless of its type. For example, if a Trojan horse or keylogger does not act maliciously, behavioral analysis does not detect it.

SONAR detects the following items:

Heuristic threats	Behavioral analysis uses heuristics to determine if an unknown file behaves suspiciously and might be a high risk or low risk. It also uses reputation data to determine whether the threat is a high risk or low risk.
System changes	Behavioral analysis detects applications or the files that try to modify DNS settings or a host file on a client computer.
Trusted applications that exhibit bad behavior	Some good trusted files might be associated with suspicious behavior. Behavioral analysis detects these files as suspicious behavior events. For example, a well-known document sharing application might create executable files.

If you disable Auto-Protect, you limit the ability for behavioral analysis to make detections of high and low risk files. If you disable Insight lookups (reputation queries), you also limit the behavioral analysis detection capability.

More information

- [Managing SONAR](#)
- [Managing exceptions in Symantec Endpoint Protection](#)

Handling and preventing behavioral analysis (SONAR) false positive detections

Behavioral analysis might make false positive detections for certain internal custom applications. Also, if you disable Insight lookups, the number of false positives from behavioral analysis increases. See:

[Understanding server data collection and client submissions and their importance to the security of your network](#)

You can change behavioral analysis settings to mitigate false positive detections in general. You can also create exceptions for a specific file or a specific application that behavioral analysis detects as a false positive.

WARNING

If you set the action for high risk detections to log only, you might allow potential threats on your client computers.

Table 111: Handling SONAR false positives

Task	Description
Log SONAR high risk heuristic detections and use application learning	You might want to set detection action for high risk heuristic detections to Log for a short period of time. Let application learning run for the same period of time. Symantec Endpoint Protection learns the legitimate processes that you run in your network. Some true detections might not be quarantined, however. See: Enabling application learning After the period of time, you should set the detection action back to Quarantine. Note: If you use aggressive mode for low risk heuristic detections, you increase the likelihood of false positive detections. Aggressive mode is disabled by default. For more information, see: Adjusting SONAR settings on your client computers
Create exceptions for SONAR to allow safe applications	You can create exceptions for SONAR in the following ways: • Use the SONAR log to create an exception for an application that was detected and quarantined You can create an exception from the SONAR log for false positive detections. If the item is quarantined, Symantec Endpoint Protection restores the item after it rescans the item in the Quarantine. Items in the Quarantine are rescanned after the client receives updated definitions. See: Creating exceptions from log events • Use an Exceptions policy to specify an exception for a particular file name, folder name, or application. You can exclude an entire folder from SONAR detection. You might want to exclude the folders where your custom applications reside. See: Creating exceptions for Virus and Spyware scans

Adjusting SONAR settings on your client computers

You might want to change the SONAR actions to reduce the rate of false positive detections. You might also want to change the SONAR actions to change the number of detection notifications that appear on your client computers.

NOTE

A cloud icon appears next to some options when this domain is enrolled in the cloud console. If an Intensive Protection policy is in effect, the policy overrides these options.

To adjust SONAR settings on your client computers

1. In the Virus and Spyware Protection policy, select **SONAR**.
2. In 14.3 RU4 or earlier, make sure that **Enable SONAR** is checked.
3. In 14.3 RU4 or earlier, under **Scan Details**, change the actions for high or low risk heuristic threats.
You can enable aggressive mode for low risk detections. This setting increases SONAR sensitivity to low risk detections. It might increase the false positive detections.
4. Optionally change the settings for the notifications that appear on your client computers.
5. Under **System Change Events**, change the action for either **DNS change detected** or **Host file change detected**.

NOTE

The **Prompt** action might result in many notifications on your client computers. Any action other than **Ignore** might result in many log events in the console and email notifications to administrators.

WARNING

If you set the action to **Block**, you might block important applications on your client computers.

For example, if you set the action to **Block** for **DNS change detected**, you might block VPN clients. If you set the action to **Block** for **Host file change detected**, you might block your applications that need to access the host file. You can use a DNS or host file change exception to allow a specific application to make DNS or host file changes.

For more information, see:

[Creating an exception for an application that makes a DNS or host file change](#)

6. Under **Suspicious Behavior Detection**, you can change the action for high or low risk detections.

7. Click **OK**.

More information

- [Managing SONAR](#)
- [Creating exceptions for Virus and Spyware scans](#)

Monitoring behavioral analysis (SONAR) detection results to check for false positives

The client collects and uploads behavioral analysis detection results to the management server. The results are saved in the SONAR log.

To determine which processes are legitimate and which are security risks, look at the following columns in the log:

Event	The event type and the action that the client has taken on the process, such as cleaning it or logging it. Look for the following event types: • A possible legitimate process is listed as a Potential risk found event. • A probable security risk is listed as a Security risk found event.
Application	The process name.
Application type	The type of malware that a behavioral analysis scan detected.
File/Path	The path name from where the process was launched.

The **Event** column tells you immediately whether a detected process is a security risk or a possible legitimate process. However, a potential risk that is found may or may not be a legitimate process, and a security risk that is found may or may not be a malicious process. Therefore, you need to look at the **Application type** and **File/Path** columns for more information. For example, you might recognize the application name of a legitimate application that a third-party company has developed.

To monitor SONAR detection results to check for false positives

1. In the console, click **Monitors > Logs**.
2. On the Logs tab, in the **Log type** drop-down list, click **SONAR**.
3. Select a time from the **Time range** list box closest to when you last changed a scan setting.
4. Click **Additional Settings**.
5. In the **Event type** drop-down list, select one of the following log events:
 - To view all detected processes, make sure **All** is selected.
 - To view the processes that have been evaluated as security risks, click **Security risk found**.
 - To view the processes that have been evaluated and logged as potential risks, click **Potential risk found**.

-
6. Click **View Log**.
 7. After you identify the legitimate applications and the security risks, create an exception for them in an Exceptions policy.

You can create the exception directly from the SONAR Logs pane.

More information

[Creating exceptions from log events](#)

Protecting Symantec Endpoint Protection processes and resources with Tamper Protection

Tampering and/or disabling security software is a technique employed by many targeted attacks in today's threat landscape. Tamper Protection is a key technology that protects Symantec Endpoint Protection processes and resources from any attempts of alteration or disabling. Tamper Protection blocks modifications to Symantec Endpoint Protection registry settings, files, and prevents tampering with running processes on Windows clients.

If you use any third-party security risk scanners that detect and defend against unwanted adware and spyware, these scanners typically affect Symantec resources. If you set Tamper Protection to log tamper events when you run such a scanner, Tamper Protection generates a large number of log entries. If you decide to log Tamper Protection events, use log filtering to manage the number of events.

You can configure the client to block or log attempts to modify Symantec resources. You can create exceptions for the applications that Tamper Protection detects.

Tamper Protection settings are configured for a selected group.

To enable or disable Tamper Protection

1. In the console, click **Clients**.
2. On the **Policies** tab, under **Settings**, click **General Settings**.
3. On the **Tamper Protection** tab, check or uncheck **Protect Symantec security software from being tampered with or shut down**.
4. In the list box under **Actions to take if an application attempts to tamper with or shut down Symantec security software**, select one of the log actions.
5. Click **OK**.

More information

[Creating a Tamper Protection exception on Windows clients](#)

Application control, system lockdown, and device control

To monitor and control the behavior of applications on client computers, you use application control and system lockdown. Application control allows or blocks the defined applications that try to access system resources on a client computer. System lockdown allows only approved applications on client computers. To manage hardware devices that access client computers, you use device control.

WARNING

Application control and system lockdown are advanced security features that only experienced administrators should configure.

You use application control, system lockdown, and device control for the following tasks.

Application control	• Prevent malware from taking over applications. • Restrict the applications that can run. • Prevent users from changing configuration files. • Protect specific registry keys. • Protect particular folders, such as \WINDOWS\system. You configure application control and device control using an Application and Device Control policy. See: Setting up application control
System lockdown	• Control the applications on your client computers. • Block almost any Trojan horse, spyware, or malware that tries to run or load itself into an existing application. System lockdown ensures that your system stays in a known and trusted state. Note: If you do not implement system lockdown carefully, it can cause serious problems in your network. Symantec recommends that you implement system lockdown in specific stages. You configure system lockdown in the Policies tab on the Clients page. See: Configuring system lockdown
Device control	• Block or allow different types of devices that attach to client computers, such as USB, infrared, and FireWire devices. • Block or allow serial ports and parallel ports. For more information, see: Managing device control

Mac computers support device control.

Setting up application control

Application control allows or blocks the defined applications that try to access system resources on a client computer. You can allow or block access to certain registry keys, files, and folders. You can also define which applications are allowed to run, which applications that cannot be terminated through irregular processes, and which applications can call DLLs.

Use the following steps to set up application control on a group of client computers.

Table 112: Setting up application control

Steps	Description
Open a policy and enable default application control rule sets	Application Control policies contain predefined rule sets, which are disabled by default. You can enable any sets that you need, and apply the policy to a group. The predefined rule sets are configured in production mode rather than test mode. However, you should change the setting to test mode and test the rules in your test network before you apply them to your production network. See: Enabling and testing default application rules
Add additional application control rules (optional)	If the default rule sets do not meet your requirements, add new rule sets and rules. Typically, only advanced administrators should perform this task. See: Adding custom rules to Application Control
Add exceptions for applications	Application control injects code in some applications to examine them, which can slow applications that run on the computer. If necessary, you can exclude some applications from application control. You use an Exceptions policy to add file exceptions or folder exceptions for application control. See: Excluding a file or a folder from scans

Steps	Description
View the Application Control logs	If you are testing a new policy or are troubleshooting an issue, you should monitor application control events in the log. In both test mode and production mode, application control events are in the Application Control log in Symantec Endpoint Protection Manager. On the client computer, application control and device control events appear in the Control log. You might see duplicate or multiple log entries for a single application control action. For example, if explorer.exe tries to copy a file, it sets the write and delete bits of the file's access mask. Symantec Endpoint Protection logs the event. If the copy action fails because an application control rule blocks the action, explorer.exe tries to copy the file by using only the delete bit in the access mask. Symantec Endpoint Protection logs another event for the copy attempt. See: Viewing logs
Prevent or allow users from enabling or disabling application control (optional)	In rare cases, application control might interfere with some safe applications that run on client computers. You might want to allow users to disable this option to troubleshoot problems. In the mixed mode or client mode, use the Allow user to enable and disable the application device control setting in the Client User Interface Settings dialog. See: Preventing users from disabling protection on client computers

You can also use system lockdown to allow approved applications or block unapproved applications on the client computers. See:

[Configuring system lockdown](#)

Enabling and testing default application rules

Application control includes default rule sets that are made up of one or more rules. Default application control rule sets are installed with the Symantec Endpoint Protection Manager. The default rule sets are disabled at installation. To use the default rule sets in an Application Control policy, you must enable them and apply the policy to a group of clients.

For a description of the common predefined rules, see:

[Hardening Symantec Endpoint Protection \(SEP\) with an Application and Device Control Policy to increase security](#)

In the following task you can enable and test the **Block writing to USB drives** rule set.

To enable a default application rule set

1. In the console, click **Policies > Application and Device Control**, and under **Tasks**, click **Add an Application Control Policy**.
2. In the **Overview** pane, type a name and description for the policy.
3. Click **Application Control**.
4. In the **Application Control** pane, check the **Enabled** check box next to each rule set that you want to implement. For example, next to the **Block writing to USB drives** rule set, check the check box in the Enabled column.
5. To review the rules for the rule set, select the rule, click **Edit**, and then click **OK**.
[Adding custom rules to Application Control](#)
6. Change **Production** to **Test (log only)**.
7. Assign the policy to a group, and click **OK**.

To test the rule set Block writing to USB drives

1. On the client computer, attach a USB drive.
2. Open Windows Explorer and double-click the USB drive.
3. Right-click the window and click **New > Folder**.
If application control is in effect, an **Unable to create folder** error message appears.

More information

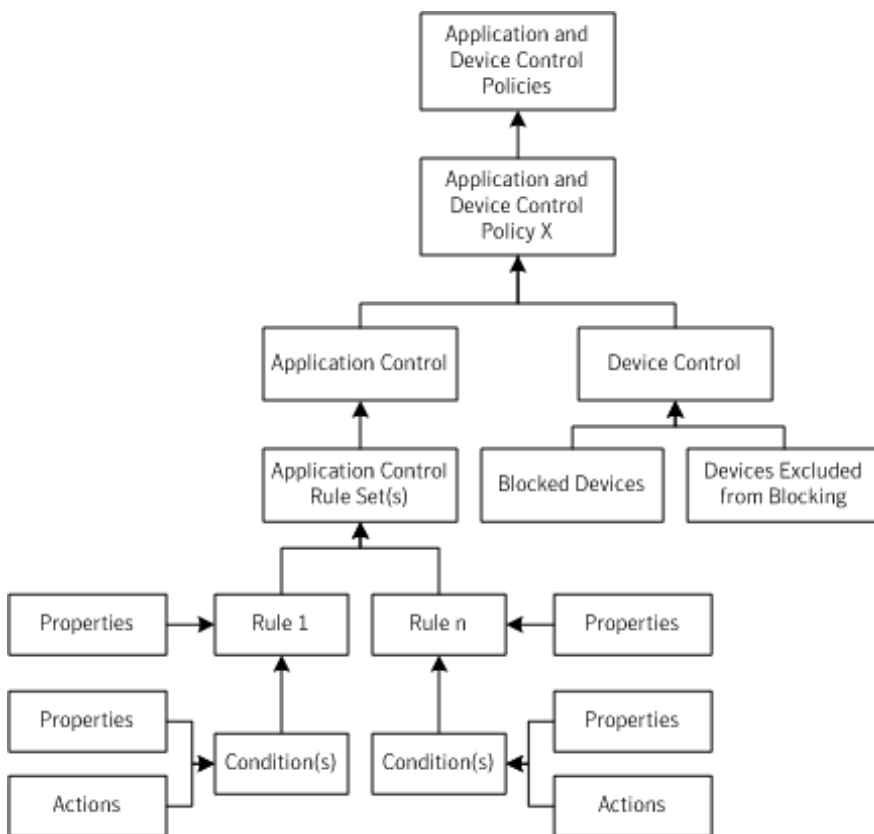
- [About application control, system lockdown, and device control](#)
- [About the structure of an Application Control and Device Control policy](#)

The structure of an Application Control and Device Control policy

The Application and Device Control policy has two parts:

- Application Control contains one or more rule sets. Each rule set contains one or more rules. You configure properties, conditions, and actions for each rule:
 - **Rules** define the application(s) that you want to monitor.
 - **Conditions** monitor specified operations for the application(s) defined in the rule. The condition also contains the actions to take when the specified operation is observed.
 - As you add the rules and conditions, you need to specify the specific **properties** of the condition and what actions to take when the condition is met. Each condition type has different properties.
- Device control consists of a list of blocked devices and a list of devices that are excluded from blocking. You can add to these two lists and manage their contents.

The following figure illustrates the application and device control components and how they relate to each other.



More information

- [About application control, system lockdown, and device control](#)
- [Setting up application control](#)
- [Adding custom rules to Application Control](#)
- [Managing device control](#)

Adding custom rules to Application Control

If the default rule sets do not meet your requirements, add new rule sets and rules. You can also modify the predefined rule sets that are installed with the policy.

- The rule set is the container that holds one or more rules that allows or blocks an action.
- The rules in the rule sets define one or more processes or applications. You can also exclude a process from being monitored.
- Each rule includes the conditions and the actions that apply to a given process or processes. For each condition, you can configure actions to take when the condition is met. You configure rules to apply to only certain applications, and you can optionally configure them to exclude other applications from having the action applied.

[About the structure of an Application Control and Device Control policy](#)

Use the following steps to add your own application rules:

- [Step 1: Add a custom rule set and rules to an Application Control policy \(optional\)](#)
- [Step 2: Define the application or process for the rule \(optional\)](#)
- [Step 3: Add conditions and actions to a rule \(optional\)](#)
- Step 4: Test the rules before you apply them to your production network. See: [Testing application control rules](#)

Step 1: Add custom rule sets and rules to an Application Control policy (optional)

A best practice is to create a rule set that includes all of the actions that allow, block, and monitor a given task. On the other hand, you should create multiple rule sets if you have multiple tasks. For example, if you wanted to block write attempts to all removable drives and also block applications from tampering with a specific application, you should create two rules sets. You add and enable as many rule sets and rules as you need.

For example, BitTorrent is a communications protocol that is used for peer-to-peer file sharing and is not secure. BitTorrent distributes movies, games, music, and other files. BitTorrent is one of the simplest methods to distribute threats. Malware is hidden inside the files that are shared on peer-to-peer networks. You can use application control to block access to the BitTorrent protocol. You can also use peer-to-peer authentication and intrusion prevention. See:

[Blocking a remote computer by configuring peer-to-peer authentication](#)

Consider the order of the rules and their conditions when you configure them to avoid unexpected consequences. Typically, only advanced administrators should perform this task. See:

[Best practices for adding application control rules](#)

To add custom rule sets and rules to an Application Control policy

1. Open an Application Control policy. See: [Enabling and testing default application rules](#)
2. In the **Application Control** panel, under the list of default rule sets, click **Add**.
To modify a predefined rule set, select it and then click **Edit**. For example, to monitor the applications that access the BitTorrent protocol, select **Block programs from running from removable drives [AC2]**.
3. In the **Add Application Control Rule Set** dialog box, type a name and description for the rule set.
4. Under Rules, select **Rule 1**, and on the **Properties** tab, type a meaningful name and description for the rule.
To add an additional rule, click **Add > Add Rule**.

Step 2: Define the application or process for the rule (optional)

Each rule must have at least one application or process that it monitors on the client computer. You can also exclude certain applications from the rule.

To define the application or process for the rule

1. With the rule selected, on the **Properties** tab, next to **Apply this rule to the following processes**, click **Add**.
2. In the **Add Process Definition** dialog box, type the application name or process name, such as `bittorrent.exe`.
If you apply the rule to all applications except for a given set of applications, then define a wildcard for all (*) in this step. Then list the applications that need to be exceptions next to **Do not apply this rule to the following processes**.
3. Click **OK**.

The **Enable this rule** check box is enabled by default. If you uncheck this option, the rule does not apply.

Step 3: Add conditions and actions to a rule (optional)

The conditions control the behavior of the application or process that attempts to run on the client computer. Each condition type has its own properties to specify what the condition looks for.

Each condition has its own specific actions to take on the process when the condition is true. Except for the Terminate process action, the actions always apply to the process that you define for the rule, and not the condition.

WARNING

The **Terminate** process action terminates the caller process, or the application that made the request. The caller process is the process that you define in the rule and not the condition. The other actions act on the target process, defined in the condition.

Table 113: Actions taken by conditions

Condition	Description
Registry Access Attempts	Allows or blocks access to a client computer's registry settings.
File and Folder Access Attempts	Allows or blocks access to defined files or folders on a client computer.
Launch Process Attempts	Allows or blocks the ability to launch a process on a client computer.
Terminate Process Attempts	Allows or blocks the ability to terminate a process on a client computer. For example, you may want to block a particular application from being stopped. Warning! The Terminate Process Attempt condition refers to the target process. If you use the Terminate Process Attempts condition on Symantec Endpoint Protection or another important process and then use the Terminate process action to kill the process that tries to kill Symantec Endpoint Protection.
Load DLL Attempts	Allows or blocks the ability to load a DLL on a client computer.

To add conditions and actions to a rule

1. Under **Rules**, select the rule you added, click **Add > Add Condition**, and choose a condition. See: [Best practices for choosing which condition to use for a rule](#)
For example, click **Launch Process Attempts** to add a condition for when the client computer accesses the BitTorrent protocol.
2. On the **Properties** tab, select the process that should or should not be launched:
 - To specify a process to launch:
Next to **Apply to the following entity**, click **Add**.
 - To exclude a process from being launched:
Next to **Do not apply to the following processes**, click **Add**.
3. In the **Add entity Definition** dialog box, type process name, DLL, or registry key.
For example, to add BitTorrent, type its file path and executable, such as: `C:\Users\UserName\AppData\Roaming\BitTorrent`

To apply a condition to all processes in a particular folder, a best practice is to use `folder_name\*` or `folder_name\*\*`. One asterisk includes all the files and folders in the named folder. Use `folder_name\*\*` to include every file and folder in the named folder plus every file and folder in every subfolder.

4. Click **OK**.
5. On the **Actions** tab for the condition, select an action to take.
For example, to block Textpad if it tries to launch Firefox, click **Block access**.
6. Check **Enable logging** and **Notify user**, and add a message you want the client computer user to see.
For example, type `Textpad tries to launch Firefox`.
7. Click **OK**.
The new rule set appears and is configured for test mode. You should test new rule sets before you apply them to your client computers.

Best practices for adding application control rules

You should plan your custom application control rules carefully. When you add application control rules, keep in mind the following best practices.

Table 114: Best practices for application control rules

Best practice	Description	Example
Consider the rule order	Application control rules work similarly to most network-based firewall rules in that both use the first rule match feature. When multiple conditions are true, the first rule is the only one that is applied unless the action that is configured for the rule is to Continue processing other rules .	You want to prevent all users from moving, copying, and creating files on USB drives. You have an existing rule with a condition that allows write access to a file named Test.doc. You add a second condition to this existing rule set to block all USB drives. In this scenario, users are still able to create and modify a Test.doc file on USB drives. The Allow access to Test.doc condition comes before the Block access to USB drives condition in the rule set. The Block access to USB drives condition does not get processed when the condition that precedes it in the list is true.
Use the right action	The Terminate Process Attempts condition allows or blocks an application's ability to terminate the calling process on a client computer. The condition does not allow or prevent users from stopping an application by the usual methods, such as clicking Quit from the File menu.	Process Explorer is a tool that displays the DLL processes that have opened or loaded, and what resources the processes use. You might want to terminate Process Explorer when it tries to terminate a particular application. Use the Terminate Process Attempts condition and the Terminate process action to create this type of rule. You apply the condition to the Process Explorer application. You apply the rule to the application or applications that you do not want Process Explorer to terminate.
Use one rule set per goal	Create one rule set that includes all of the actions that allow, block, or monitor a given task.	You want to block write attempts to all removable drives and you want to block applications from tampering with a particular application. To accomplish these goals, you should create two different rule sets instead of one rule set.

Best practice	Description	Example
Use the Terminate process action sparingly	The Terminate process action kills the calling process when the process meets the configured condition. Only advanced administrators should use the Terminate process action. Typically, you should use the Block access action instead.	You want to terminate Winword.exe any time that any process launches Winword.exe. You create a rule and configure it with the Launch Process Attempts condition and the Terminate process action. You apply the condition to Winword.exe and apply the rule to all processes. You might expect this rule to terminate Winword.exe, but that is not what the rule does. If you try to start Winword.exe from Windows Explorer, a rule with this configuration terminates Explorer.exe, not Winword.exe. Users can still run Winword.exe if they launch it directly. Instead, use the Block access action, which blocks the target process, or Winword.exe.
Test rules before you put them into production	The Test (log only) option for rule sets logs the actions, and does not apply to the actions to the client computer. Run rules in test mode for some acceptable period of time before you switch them back to production mode. During this time period, review the Application Control logs and verify that the rules work as planned.	The test option reduces potential accidents you might make by not considering all possibilities of the rule. See: Testing application control rules

More information

- [Adding custom rules to Application Control](#)
- [Best practices for choosing which condition to use for a rule](#)

Best practices for choosing which condition to use for a rule

You add custom application control rules and conditions to prevent users from opening applications, writing to files, or sharing files. You can look at the default rule sets to help determine how to set up your rules. For example, you can edit the **Block applications from running** rule set to view how you might use a **Launch Process Attempts** condition. See:

[Adding custom rules to Application Control](#)

Table 115: Typical conditions to use for a rule

Rule	Condition
Prevent users from opening an application	You can block an application when it meets either of these conditions: • Launch Process Attempts For example, to prevent users from transferring FTP files, you can add a rule that blocks a user from launching an FTP client from the command prompt. • Load DLL Attempts For example, if you add a rule that blocks Msvcr7.dll on the client computer, users cannot open Microsoft WordPad. The rule also blocks any other application that uses the DLL.
Prevent users from writing to a particular file	You may want to let users open a file but not modify the file. For example, a file may include the financial data that employees should view but not edit. You can create a rule to give users read-only access to a file. For example, you can add a rule that lets you open a text file in Notepad but does not let you edit it. Use the File and Folder Access Attempts condition for this type of rule.

Rule	Condition
Block file shares on Windows computers	You can disable local file and print sharing on Windows computers. Include the following conditions: • Registry Access Attempts Add all the relevant Windows security and sharing registry keys. • Launch Process Attempts Specify the server service process (svchost.exe). • Load DLL Attempts Specify the DLLs for the Security and Sharing tabs (rshx32.dll, ntshrui.dll). • Load DLL Attempts Specify the server service DLL (srvsvc.dll). You set the action for each condition to Block access. You can also use firewall rules to prevent or allow client computers to share files. See: Permitting clients to browse for files and printers in the network
Prevent users from running peer-to-peer applications	You can prevent users from running peer-to-peer applications on their computers. You can create a custom rule with a Launch Process Attempts condition. In the condition, you must specify all peer-to-peer applications that you want to block, such as LimeWire.exe or *.torrent. You can set the action for the condition to Block access. Use an Intrusion Prevention policy to block network traffic from peer-to-peer applications. Use a Firewall policy to block the ports that send and receive peer-to-peer application traffic. See: • Managing intrusion prevention • Creating a firewall policy
Block write attempts to DVD drives	Currently, application control does not have a default rule that blocks CD/DVD writing directly. Instead, you create a rule that blocks the specific DLLs that write to CD or DVD drives using the Add Condition and File and Folder Access Attempts conditions. You should also create a Host Integrity policy that sets the Windows registry key to block write attempts to DVD drives. See: • Setting up Host Integrity • How to block CD/DVD Writing in Windows 7

Testing application control rules

After you add application control rules, you should test them in your network. Configuration errors in the rule sets that are used in an Application Control policy can disable a computer or a server. The client computer can fail, or its communication with Symantec Endpoint Protection Manager can be blocked. After you test the rules, apply them to your production network.

Step 1: Set the rule set to test mode

You test rule sets by setting the mode to test mode. Test mode creates a log entry to indicate when rules in the rule set would be applied without actually applying the rule.

Default rules use production mode by default. Custom rules use test mode by default. You should test both default and custom rules sets.

You might want to test rules within the set individually. You can test individual rules by enabling or disabling them in the rule set.

To change a rule set to test mode

-
1. In the console, open an Application and Device Control policy.
 2. Under **Application Control Policy**, click **Application Control**.
 3. In the **Application Control Rule Sets** list, click the drop-down arrow in the **Test/Production** column for the rule set, and click **Test (log only)**.

For more information, see:

[Setting up application control](#)

Step 2: Apply the Application and Device Control policy to computers in your test network

If you created a new Application and Device Control policy, apply the policy to clients in your test network. See:

[Assigning a policy to a group or location](#)

Step 3: Monitor the Application Control log

After you run your rule sets in test mode for a period of time, check the logs for any errors. In both test mode and production mode, application control events are in the Application Control log in Symantec Endpoint Protection Manager. On the client computer, application control and device control events appear in the Control log.

You might see duplicate or multiple log entries for a single application control action. For example, if explorer.exe tries to copy a file, it sets the write and delete bits of the file's access mask. Symantec Endpoint Protection logs the event. If the copy action fails because an application control rule blocks the action, explorer.exe tries to copy the file by using only the delete bit in the access mask. Symantec Endpoint Protection logs another event for the copy attempt. See:

[Viewing logs](#)

Step 4: Change the rule set back to production mode

When the rules function like you expect them to, change the rule set back to production mode.

Configuring system lockdown

System lockdown controls which applications are allowed to run on client computers by using an allow list or a deny list.

- The allow list (whitelist) includes all the approved applications. The clients block all other applications.
- The deny list (blacklist) includes all the unapproved applications. The clients allow all other applications.

You should generate a list of all the applications that the client runs. For example, your network might include Windows 8.1 32-bit and 64-bit clients, and Windows 10 64-bit clients. You can create a file fingerprint list for each client image.

You can create an allow list or deny list by generating a list of either file fingerprints or specific application filenames:

- The *file fingerprint list* includes file fingerprints and computer path locations. Using the file fingerprint list is more secure than using the application names, because a hacker can rename the application name.
- The *filename list* includes the file path and the application name, such as `C:\Program Files\Notepad++`. The filename list is easier to maintain. If a well-known application that you allow updates often, you do not have to constantly update the file fingerprint list.

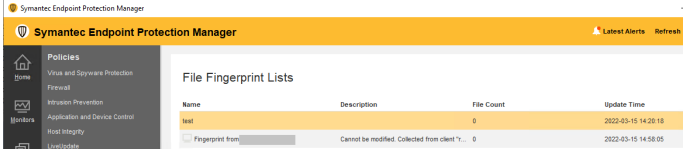
NOTE

- You set up system lockdown for each group or location in your network.
- Any applications that system lockdown allows are subject to other protection features in Symantec Endpoint Protection.
- You can use an Application Control policy to control specific applications instead of or in addition to system lockdown.

System lockdown steps

NOTE

The Application Control component must be installed and enabled for system lockdown to work.

Action	Description
Step 1: Create a file fingerprint list or filename list.	Method 1: Creating a file fingerprint list You create a file fingerprint list using one of the following methods: - The checksum.exe utility that is installed with the client software. The checksum.exe utility collects all the fingerprints for the applications in a specified path. This method is useful for creating a deny list. - The Collect File Fingerprint List command. This command collects a file fingerprint list that includes every application on the targeted client group or individual client computer. This method is useful for creating an allow list. You cannot modify the file fingerprint list that the command generates. Skip Step 2 and go to Step 3 if you use this method. - A third-party scripting tool, such as PowerShell or Python, or a text editor. The checksum.exe utility (as of 14.3 RU5) and the Collect File Fingerprint List command (as of 14.3 RU5) create a list with both the legacy MD5 and the more secure SHA-256 file fingerprints. For more information, see: Creating a file fingerprint list Note: If you run Symantec EDR in your network, you might see file fingerprint lists from Symantec EDR. For more information, see: Note: Interaction between system lockdown and Symantec EDR deny list (blacklist) rules Method 2: Creating a filename list Alternatively, you can add individual application names to a filename list to allow or block them. You can use any text editor to create a text file that includes the filenames. Unlike file fingerprint lists, you add or import these filenames directly into the system lockdown configuration. After you import the filenames, the applications appear as individual entries in the system lockdown configuration. If you add the filenames directly, you get an expanded set of attributes with which to monitor the application. Skip Step 2 and go to Step 3 if you use this method. Note: Having a large number of named applications might affect client computer performance when system lockdown is enabled in deny mode. For more information, see: Creating an application name list to import into the system lockdown configuration
Step 2: Import file fingerprint lists into Symantec Endpoint Protection Manager (using checksum.exe or a third-party fingerprint generation tool only).	If you generate the file fingerprint list in Step 1 using the checksum.exe or a third-party fingerprint generation utility, add the list to Policies > Policy Components > File Fingerprint Lists.  For more information, see: Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager Note: If you use the Collect File Fingerprint List command, the list is automatically added.

Action	Description
Step 3: Allow or block the file fingerprint list or filename list.	By default, system lockdown is disabled and allows all applications. All applications are logged but not blocked. To allow or block the applications • In the System Lockdown dialog box, click Log Unapproved Applications Only. • Click Allow Mode or Deny Mode. – In allow mode (the default), the file fingerprints are approved applications. When you enable system lockdown in allow mode, you block any application that is not on the approved applications list. – In deny mode, the file fingerprints are unapproved applications. When you enable system lockdown in deny mode, you block any application that is on the unapproved applications list. • Add either the file fingerprint list and/or individual applications to the system lockdown configuration. You can import a list of application names rather than enter the names individually in the system lockdown configuration. – In allow mode, the applications are approved applications. – In deny mode, the applications are unapproved applications. • Click OK to run the test for a period of time. For more information, see: Setting up and testing the system lockdown configuration before you enable system lockdown
Step 4: View the unapproved applications and modify the system lockdown configuration if necessary.	After you run the test for a period of time, you can check the list of unapproved applications. You can view the list of unapproved applications by checking the status in the System Lockdown dialog box. The logged events also appear in the Application Control log. You can decide whether to add more applications to the file fingerprint list or the applications list. You can also add or remove file fingerprint lists or applications if necessary before you enable system lockdown. For more information, see: Setting up and testing the system lockdown configuration before you enable system lockdown
Step 5: Enable system lockdown.	To enable system lockdown • In the System Lockdown dialog box, click Enable System Lockdown. • Click OK. Note: Make sure that you test your configuration before you enable system lockdown. If you block a needed application, your client computers might be unable to restart.

Optional testing steps

Action	Description
Step 1: Update file fingerprint lists for system lockdown.	Over time, you might change the applications that run in your network. You can update your file fingerprint lists or can remove lists as necessary. You can update file fingerprint lists in the following ways: • Manually append, replace, or merge file fingerprint lists that you imported. You cannot append file fingerprint lists to a fingerprint list that you generate with the Collect File Fingerprint List command. You can append an imported list with a command-generated list. In that case, if you re-run the fingerprint command, you must recreate the appended list. For more information, see: – Manually updating a file fingerprint list in Symantec Endpoint Protection Manager – Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager • Automatically update existing file fingerprint lists that you imported. You can also automatically update applications or the application name lists that you import. For more information, see: Automatically update file fingerprint lists to allow or block for system lockdown • Re-run the Collect File Fingerprint List command to automatically update a command-generated fingerprint list. For more information, see: Creating a file fingerprint list When you re-run the command, the new list automatically replaces the existing list. Note: You might want to re-test the entire system lockdown configuration if you add client computers to your network. You can move new clients to a separate group or test network, and then disable system lockdown. Or you can keep system lockdown enabled and run the configuration in log-only mode. You can also test individual file fingerprints or applications as described in Step 2.
Step 2: Test selected items before you add or remove them when system lockdown is enabled.	After system lockdown is enabled, you can test individual file fingerprints, application name lists, or specific applications before you add or remove them to the system lockdown configuration. If you have file fingerprint lists that you no longer use, consider removing them. Note: Be careful when you add or remove a file fingerprint list or a specific application from system lockdown. Adding or removing items from system lockdown can be risky. You might block important applications on your client computers. • Test selected items. Use the Test Before Removal option to log specific file fingerprint lists or specific applications as unapproved. When you run this test, system lockdown is enabled but does not block any selected applications or any applications in the selected file fingerprint lists. Instead, system lockdown logs the applications as unapproved. • Check the Application Control log. The log entries appear in the Application Control log. If the log has no entries for the tested applications, you know that your clients do not use those applications.

More information

[Setting up application control](#)

Creating a file fingerprint list

You can use either the **Collect File Fingerprint List** command or the checksum.exe utility to create a file fingerprint list.

The file fingerprint list contains the following items for each executable file or DLL that resides in a specified path on the computer:

- The path
- The file name
- The corresponding fingerprint

You then import the file fingerprint list into Symantec Endpoint Protection Manager to use in your system lockdown configuration.

For more information, see:

- [Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager](#)
- [Configuring system lockdown](#)
- [Best practices for importing file fingerprint lists for SEP 14.3 RU5 and later](#)

You can also use a third-party scripting tool to create a file fingerprint list.

Table 116: File fingerprint example output

Fingerprint type	Example
MD5 14.3 RU4 and earlier	bbe80313cf12098d3fc4d8a42e9dbb33 c:\Windows\System32\notepad.exe
MD5 and SHA-256 14.3 RU5 and later	bbe80313cf12098d3fc4d8a42e9dbb33, deb5b0067e4af84bb0 7fa3d84631cee94787fb3be7cda11c0016992f54ab4dda c:\Windows\System32\notepad.exe

NOTE

A SEPM 14.3 RU5 and later can collect both MD5 and SHA-256 file fingerprints on 14.3 RU4 clients.

Using the Collect File Fingerprint List command

You cannot modify the file fingerprint list that the command generates.

The SEPM 14.3 RU5 or later **Collect File Fingerprint List** command creates a list that includes both the legacy MD5 and the more secure SHA-256 file fingerprints.

Mac and Linux client computers do not process this command.

NOTE

The command does not generate the corresponding directory paths and file names.

To create a file fingerprint list with the Collect File Fingerprint List command

1. On the **Clients** page, right-click a group or an individual client, and then select **Collect File Fingerprint List**.
When you run this command, the file fingerprint list is automatically imported into **Policies > Policy Components > File Fingerprint Lists**.

For more information, see:

[Running commands on client computers from the console](#)

Using the checksum.exe utility

The checksum.exe utility is installed with the Symantec Endpoint Protection client computer.

- The 14.3 RU5 and later checksum.exe utility creates a list that includes both the legacy MD5 and the SHA-256 file fingerprints. You can run this command with or without the `csv` switch.
- The 14.3 RU4 and earlier checksum.exe utility creates a list with the MD5 and the SHA-256 file fingerprints *with* the `csv` switch.
- The 14.3 RU4 and earlier checksum.exe utility creates a list with the MD5 file fingerprints and filenames *without* the `csv` switch.

NOTE

A SEPM 14.3 RU5 and later can collect both MD5 and SHA-256 file fingerprints on 14.3 RU4 clients.

To create a file fingerprint list with checksum.exe utility

1. Open a command prompt window on the computer that contains the image for which you want to create a file fingerprint list.

The computer must have Symantec Endpoint Protection client software installed.

2. Navigate to the client installation folder, which contains the checksum.exe file. Typically, the file is located in the following folder:

On 32-bit computers: `C:\Program Files\Symantec\Symantec Endpoint Protection\`

On 64-bit computers (14.3 RU4 and earlier): `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\`

On 64-bit computers (14.3 RU5 and later): `C:\Program Files\Symantec\Symantec Endpoint Protection\`

3. Type either one the following commands:

- `checksum.exe <outputfile.txt> <path>`
- `checksum.exe <outputfile.txt> -csv <path>` (with the `csv` switch)

Where:

- `<outputfile.txt>` is the name of the resulting text file that contains the fingerprints for all the applications that are located on the specified drive.
- `<path>` is the file path on the computer on which you want to gather fingerprint information.
- The `csv` switch is not case-sensitive.

NOTE

To run the checksum.exe utility against all files on the C drive, you must add a forward slash at the end of `<path>`. Otherwise, the command only runs in the folder where `checksum.exe` is located.

The format of each line in the output file can be either one of the following:

`fingerprint_of_the_file full_pathname_of_the_exe_or_DLL`

`fingerprint_of_the_file -csv full_pathname_of_the_exe_or_DLL`

4. A space separates the fingerprint value and the full pathname.

Syntax examples for checksum.exe

The following is an example of the syntax you can use to create a fingerprint list for all the files on the C drive:

```
checksum.exe cdrive.txt -csv c:/
```

This command creates a file that is called `cdrive.txt`. The file contains the fingerprints and file paths of all the executables and DLLs found on the C drive of the computer on which it runs.

NOTE

If the paths contain a space or if you use a batch file, enclose the paths with quotes (""). For example: `"C:`

`\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" cdrive.txt -csv c:/`

The following is an example of the syntax that you can use to create a fingerprint for a folder on the client computer:

```
checksum.exe blocklist.txt -csv c:\Files
```

This command creates a file that is called `blocklist.txt`. The file contains the fingerprints and file paths of any executables and DLLs found in the `Files` folder.

NOTE

If the paths contain a space or if you use a batch file, enclose the paths with quotes ("). For example: "c:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" blocklist.txt -csv "c:\Files with a space"

Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager

When you create file fingerprint lists with the `checksum.exe` utility or a third-party fingerprint generation tool, you must manually import the lists. You can also merge file fingerprint lists.

File fingerprint lists must be available in the Symantec Endpoint Protection Manager console so that you can add them to the system lockdown configuration.

For more information, see:

[Creating a file fingerprint list with checksum.exe](#)

[Best practices for importing file fingerprint lists for SEP 14.3 RU5 and later](#)

File fingerprint lists that you create with the **Collect File Fingerprint List** command become automatically available in the Policy Components page. You do not need to import them. You cannot modify file fingerprint lists that you create with the **Collect File Fingerprint List** command. You can, however, merge a command-generated file fingerprint list with another file fingerprint list. If you run the command again to regenerate the list, you must manually merge the lists again.

To import or merge file fingerprint lists

1. In the console, click **Policies**.
2. Under **Policies**, expand **Policy Components**, and then click **File Fingerprint Lists**.
3. Under **Tasks**, click **Add a File Fingerprint List**, and then click **Next**.
4. In the **Add File Fingerprint List** dialog box, click **Next**.
5. In the **Information about New File Fingerprint List** panel, type a name and description for the new list, and then click **Next**.
6. In the **Create a File Fingerprint List** panel, select one of the following options, and then click **Next**:
 - **Create the file fingerprint by importing a file fingerprint file**
Specify the path to the file fingerprint that you created. You can browse to find the file.
 - **Create the file fingerprint by combining multiple existing file fingerprints**
Select the fingerprint lists that you want to merge.

NOTE

This option is only available if you have already imported multiple file fingerprint lists.

7. Follow the onscreen instructions.
The imported or merged fingerprint lists appear under **Policies > Policy Components > File Fingerprint Lists**.

Best practices for importing file fingerprint lists for SEP 14.3 RU5 and later

When you upgrade Symantec Endpoint Protection Manager (SEPM) to 14.3 RU5 and later, Symantec recommends that you regenerate and reimport all your existing file fingerprint lists that are already assigned to a system lockdown configuration.

Starting in 14.3 RU5, both the `checksum.exe` utility and the **Collect File Fingerprint List** command generate a CSV text file that includes both the more cryptographically secure SHA-256 fingerprints and the legacy MD5 fingerprints. You may

still use file fingerprint lists containing only MD5 values, but it is not as secure. The use of the SHA-256 format eliminates the risk of a fingerprint collision attack. You can also use a file fingerprint list of SHA-256 values only, but you cannot deploy the list to 14.3 RU3 and earlier clients.

Each row of the CSV file maps the application with the MD5 file fingerprint and the corresponding SHA-256 fingerprint. There may be cases where the SHA-256 file value or the MD5 value is missing, which is called a partial mapping. This partial mapping can occur when an application is no longer on a legacy computer. If the fingerprint file list has a partial mapping, the **Policy Components > File Fingerprints Lists** page displays the following message:

```
The imported file fingerprint list contains at least one entry that uses
the legacy MD5 fingerprint type without a mapping to a more secure SHA-256
fingerprint type. Symantec recommends that you reimport a new .CSV file that
contains both MD5 and SHA-256 file fingerprints.
```

To work around this issue, regenerate the file fingerprint list using a newer client that supports SHA-256 format or manually add the missing file fingerprint. If you cannot find the missing file fingerprint:

- For a missing MD5 fingerprint, 14.3 RU4 and earlier clients ignore the application. 14.3 RU5 and later clients use the SHA-256 fingerprint.
- For a missing SHA-256 fingerprint, 14.3 RU5 and later clients use the MD5 fingerprint but are less secure.

NOTE

A SEPM 14.3 RU5 and later can collect both MD5 and SHA-256 file fingerprints on 14.3 RU4 clients.

After you regenerate the file fingerprint list for each group, you must reimport the list and retest the system lockdown configuration.

Table 117: File fingerprint example output

Fingerprint type	Example
MD5 14.3 RU4 and earlier	bbe80313cf12098d3fc4d8a42e9dbb33 c:\Windows\System32\notepad.exe
MD5 and SHA-256 14.3 RU5 and later	bbe80313cf12098d3fc4d8a42e9dbb33, deb5b0067e4af84bb0 7fa3d84631cee94787fb3be7cda11c0016992f54ab4dda c:\Windows\System32\notepad.exe

For more information, see:

[Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager](#)

[Configuring system lockdown](#)

Updating a file fingerprint list in Symantec Endpoint Protection Manager

You might want to update your file fingerprint lists after you run system lockdown for a while. You can append, replace, or remove entries in an existing file fingerprint list that you imported. You cannot directly edit any existing file fingerprint list in Symantec Endpoint Protection Manager.

If you want to merge fingerprint lists into a new list with a different name, use the **Add a File Fingerprint Wizard**.

If you create a fingerprint list with the Collect File Fingerprint List command, you cannot append, replace, or remove the entries. You can, however, append a command-generated list to an imported list. If you re-run the command, you must manually update the fingerprint list again.

You cannot modify any file fingerprint list that Symantec EDR sends to Symantec Endpoint Protection Manager. See:

-
- [Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager](#)
 - [Configuring system lockdown](#)
 - [Best practices for importing file fingerprint lists for SEP 14.3 RU5 and later](#)

To update a file fingerprint list in Symantec Endpoint Protection Manager

1. In the console, click **Policies**.
2. Under **Policies**, expand **Policy Components**, and then click **File Fingerprint Lists**.
3. In the **File Fingerprint Lists** pane, select the fingerprint list that you want to edit.
4. Click **Edit**.
5. In the **Edit File Fingerprint Wizard**, click **Next**.
6. Do one of the following:
 - Click **Append a fingerprint to this file fingerprint list** to add a new file to an existing one.
 - Click **Append other file fingerprint lists to this file fingerprint list** to merge file fingerprint lists that you already imported.
 - Click **Replace this fingerprint list with a fingerprint list file**.
 - Click **Remove all fingerprints that already appear in a fingerprint file**.
7. Do one of the following tasks:
 - Click **Browse** to locate the file or type the full path of the file fingerprint list that you want to append, replace, or remove.
 - Select the file fingerprints that you want to merge.
8. Click **Next > Close > Finish**.

Interaction between system lockdown and Symantec EDR deny list (blacklist) rules

If your network includes Symantec EDR, you might see blocked applications in the system lockdown configuration from Symantec EDR.

Symantec EDR deny lists (blacklists) interact with the system lockdown configuration in the following ways:

- When Symantec Endpoint Protection Manager receives a deny list rule from Symantec EDR, Symantec Endpoint Protection Manager enables system lockdown in deny mode for all domains and groups.
- The deny list rule appears in the Symantec Endpoint Protection Manager file fingerprint list in the system lockdown configuration. You cannot modify a file fingerprint list from Symantec EDR.
- If you configured a client group with system lockdown enabled in allow mode, the setting is preserved and Symantec Endpoint Protection Manager does not use the Symantec EDR deny list rule.
- If you disable system lockdown and delete the Symantec EDR deny list, Symantec Endpoint Protection Manager automatically re-enables system lockdown and applies the deny list.
- If you disable system lockdown but do not delete the Symantec EDR deny list, system lockdown remains disabled until you re-enable it.

NOTE

Symantec EDR sends allow list rules directly to Symantec Endpoint Protection clients. Symantec EDR does not send allow list file fingerprints to Symantec Endpoint Protection Manager.

More information

- [Configuring system lockdown](#)
- [Configuring client groups to use private servers for reputation queries and submissions](#)

Creating an application name list to import into the system lockdown configuration

You can import a list of application names into the system lockdown configuration. You might want to import an application name list rather than adding application names individually to the system lockdown configuration.

By default, 512 is the maximum number of applications that you can include in your combined application name lists. You can change the maximum in the `conf.properties` file.

You can create an application name list file with any text editor.

Each line of the file can contain the following items each separated by a space:

- The file name
If you use a path name, it must be in quotes.
- The test mode
The value should be 1 or Y for enabled or 0 or N for disabled. If you leave the field blank, test mode is disabled. You must include a value if you want to specify the matching mode.
- The matching mode (wildcard or regular expression)
The value should be 1 or Y for regular expression matching or 0 or N for wildcard matching. If you leave the field blank, wildcard matching is used.

NOTE

The test mode field enables or disables the **Test Before Addition** or **Test Before Removal** option for each application in the list. The test mode field is ignored when you use the **Log Applications Only** option to test the entire system lockdown configuration.

Each line should use the following syntax:

```
filename test_mode matching_mode
```

For example:

```
aa.exe
bb.exe 0 1
cc.exe 1
dd.exe 1 0
"c:\program files\ee.exe" 0 0
```

When you import this list into system lockdown, the individual applications appear in the system lockdown configuration with the following settings:

Table 118: Example matching mode settings

Application Name	Test Before Addition or Test Before Removal	Matching Mode
aa.exe	Disabled	Wildcard
bb.exe	Disabled	Regular expression
cc.exe	Enabled	Wildcard
dd.exe	Enabled	Wildcard
c:\program files\ee.exe	Disabled	Wildcard

More information

[Configuring system lockdown](#)

Automatically update file fingerprint lists to allow or block for system lockdown

Symantec Endpoint Protection Manager can automatically update existing file fingerprint lists and application name lists that you imported, merged, or appended.

File fingerprint lists that you generate from the **Collect File Fingerprint List** command are automatically updated when you re-run the command on the same computer.

NOTE

Starting in 14.3 RU5, both the checksum.exe utility and the **Collect File Fingerprint List** command generate a CSV text file that includes both the more cryptographically secure SHA-256 fingerprints and the legacy MD5 fingerprints. See:

[Best practices for importing file fingerprint lists for SEP 14.3 RU5 and later](#)

You can also manually update existing file fingerprints.

Table 119: Updating the allow list (whitelist) and deny list (blacklist) for system lockdown

Step	Description
Step 1: Create updated file fingerprint lists or application name lists and compress the files	You can use the checksum.exe utility or any third-party utility to create the updated file fingerprint lists. You can use any text editor to update application name lists. The lists must have the same names that already exist in Symantec Endpoint Protection Manager. See: Creating a file fingerprint list with checksum.exe A fingerprint list that you generate from the Collect File Fingerprint List command cannot be updated directly. You can merge a command-generated list with another list, or append an imported list with a command-generated list. The automatic updates feature requires a compressed file (zip file) of the file fingerprint and application name lists. You can use the file compression feature in Windows or any compression utility to zip the files.
Step 2: Create an index.ini file	The index.ini file specifies which file fingerprint lists and application names lists Symantec Endpoint Protection Manager should update. You can create an index.ini file with any text editor and copy the file to the specified URL. See: Creating an index.ini file for automatic updates of allow lists and deny lists that are used for system lockdown
Step 3: Make the compressed file and index.ini available to Symantec Endpoint Protection Manager	Symantec Endpoint Protection Manager uses UNC, FTP, or HTTP/HTTPS to retrieve the index.ini file and zip file at the specified URL. Symantec Endpoint Protection Manager uses the instructions in the index.ini file to update the specified files. When you enable automatic updates, Symantec Endpoint Protection Manager periodically checks the URL for updated files based on the schedule you set. For UNC, only JCFIS shares are supported. DFS shares are not supported. Note: If you cannot use UNC, FTP, or HTTP/HTTPS, you can copy the index.ini and updated file fingerprint and application name files directly into the following folder: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\WhitelistBlacklist\content. The files should be unzipped. Symantec Endpoint Protection Manager checks this folder if it cannot use UNC, FTP, or HTTP/HTTPS to update the files.
Step 4: Enable automatic allow list and deny list updates in the management console	You must enable the automatic update of existing allow lists or deny lists in the Symantec Endpoint Protection Manager console. You use the File Fingerprint Update dialog in Symantec Endpoint Protection Manager to enable the update feature and specify the schedule and the URL information. See: Enabling automatic updates of allow lists and deny lists for system lockdown

Step	Description
Step 5: Check the status of automatic updates for the allow list or deny list	You can make sure that Symantec Endpoint Protection Manager completes the updates by checking the status in the console. In the console, do one of the following actions: - On the Admin tab, select the site. A message appears similar to the following message: Update allow and deny lists for revision 20200528 R016 description succeeded. - On the Monitors tab, view System Logs: Server Activity. The event type typically appears similar to File fingerprint update. - On the Policies tab, under Policy Components, check the file fingerprint list description. The description appears similar to Revision: 20200528 R016 description.

More information

- [Manually updating a file fingerprint list in Symantec Endpoint Protection Manager](#)
- [Configuring system lockdown](#)

Creating an index.ini file for automatic updates of allow lists and deny lists that are used for system lockdown

The automatic updates feature requires an index.ini file. You can create the file with any text editor.

NOTE

If you use non-English characters in the text file, you should use UTF-8 without a byte order mark (BOM) character to edit and save the file.

The index.ini file specifies the following items:

- The revision and name of the compressed file that includes your updated file fingerprint lists and application name lists.
- The names of the file fingerprint lists and application name lists that you want to update.
- The names of the client groups that use the application name lists.

The existing file fingerprint list or group must currently exist in Symantec Endpoint Protection Manager. The group must have system lockdown enabled. The file fingerprint lists and application name lists must be available in the specified compressed file.

You must structure the index.ini file with the following syntax:

```
[Revision]
Revision=YYYYMMDD RXXX
SourceFile=zip file name
Description=optional description

[FingerprintList - domain name or Default]
existing fingerprint list="updated list" REPLACE/APPEND/REMOVE

[ApplicationNameList - domain name or Default]
existing group path="updated list" REPLACE/APPEND/REMOVE
```

For example, you could use the following lines in an index.ini file:

```
[Revision]
Revision=20111014 R001
SourceFile=20110901 R001.zip
Description=NewUpdates

[FingerprintList - Default]
```

```
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE
[ApplicationNameList - Default]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE
[FingerprintList - DomainABC]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE
[ApplicationNameList - DomainABC]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE
```

More information

- [Automatically update file fingerprint lists to allow or block for system lockdown](#)
- [Creating an application name list to import into the system lockdown configuration](#)

Enabling automatic updates of allow lists and deny lists for system lockdown

You can configure Symantec Endpoint Protection Manager to automatically update allow lists (whitelists) and deny lists (blacklists) that you use for system lockdown.

To automatically update a file fingerprint list that you generated with the **Collect File Fingerprint List** command, first run the command.

To enable automatic updates of allow lists and deny lists for system lockdown

1. In the console, on the **Admin** tab, click **Servers**.
2. Right-click the relevant server, and select **Edit the server properties**.
3. In the **Server Properties** dialog box, select the **File Fingerprint Update** tab.
4. On the **File Fingerprint Update** tab, check **Automatically update the allow or deny lists**.
5. Enter the URL for the location of the index.ini and the compressed file.

If you want to use UNC or FTP, you must also specify a user name and password for both the index.ini and the content.

6. Under **Schedule**, you can specify how often Symantec Endpoint Protection Manager should try to update the list.
7. Click **OK**.

More information

[Automatically update file fingerprint lists to allow or block for system lockdown](#)

Troubleshooting file fingerprint list certificate issues

Condition

If you see the following message when you upgrade Symantec Endpoint Protection Manager, the upgrade is blocked until you resolve the issue for automatically updating file fingerprint lists.

The file fingerprint list server's certificate could not be validated.

Cause/Remedy

This issue occurs when the URL of the server that automatically uploads and hosts the index.ini file sends a certificate that uses the HTTPS protocol. The HTTPS certificate may have any one of the following issues.

Cause	Remedy
The certificate expired.	Renew the expired certificate.
The certificate is self-signed.	Check that the SEPM computer trusts the certificate.
The host name of the configured URL does not match any host names in the Subject Alternate Name (SAN) attribute.	The SAN attribute lets you specify host names to be protected by an SSL certificate. For example, if you use https://mycorp.com as the server URL, when the client validates this certificate, it checks whether the mycorp.com host name is in the SAN. If you use https://192.128.100.100 as the server URL and the server sends a certificate that does not include 192.128.100.100 in the SAN attribute, the connection fails. Therefore, do one of the following tasks: • Make sure that the host name (IP address, DNS names, and so forth) of the configured server URL is a SAN attribute. A server is often reachable by using multiple host names. • Issue a new certificate for this server that lists the host name in the SAN.

Setting up and testing the system lockdown configuration before you enable system lockdown

Typically, you run system lockdown in test mode for a week, or enough time for clients to run their typical applications. After you determine that your system lockdown settings do not cause problems for users, you can enable system lockdown.

When you run system lockdown in test mode, system lockdown is disabled. System lockdown does not block any applications. Instead, unapproved applications are logged rather than blocked so that you can review the list before you enable system lockdown. You can view the log entries in the Control log. You can also view the unapproved applications in the **System Lockdown** dialog box.

NOTE

You can also create firewall rules to allow approved applications on the client.

To set up and test the system lockdown configuration before you enable system lockdown

1. In the console, click **Clients**, then under **Clients**, locate the group for which you want to set up system lockdown.
2. On the **Policies** tab, click **System Lockdown**.
3. Click **Log Unapproved Applications Only** to run system lockdown in test mode.
This option logs the unapproved applications that clients are currently running.
4. Select **Allow Mode** or **Deny Mode**.
These options changed from **Whitelist Mode** or **Blacklist Mode** in 14.3 RU1.
5. Under **Application File Lists**, under **File Fingerprint List**, add or remove file fingerprint lists.
To add a list, the list must be available in Symantec Endpoint Protection Manager. See: [Importing or merging file fingerprint lists in Symantec Endpoint Protection Manager](#)
6. To add an application name list, under **Application File Lists**, under **File Name**, click **Import**.
Specify the application name list that you want to import and click **Import**. The applications in the list appear as individual entries in the system lockdown configuration.
The application name list must be a text file that specifies the file name, test mode, and matching mode. See: [Creating an application name list to import into the system lockdown configuration](#)
7. To add an individual application, under **Application File Lists**, under **File Name**, click **Add**.
8. In the **Add File Definition** dialog box, specify the full path name of the file (.exe or .dll).

Names can be specified using a normal string or regular expression syntax. Names can include wildcard characters (* for any characters and ? for one character). The name can also include environment variables such as %ProgramFiles% to represent the location of your Program Files directory or %windir% for the Windows installation directory.

9. Either leave **Use wildcard matching (* and ? supported)** selected by default, or click **Use regular expression matching** if you used regular expressions in the file name instead.
10. If you want to allow the file only when it is executed on a particular drive type, click **Only match files on the following drive types**.
Unselect the drive types you do not want to include. By default, all drive types are selected.
11. If you want to match by device ID type, check **Only match files on the following device id type**, and then click **Select**.
12. Click the device you want in the list, and then click **OK**.
13. Click **OK** to start the test.

After a period of time, you can view the list of unapproved applications. If you re-open the **System Lockdown for name of group** dialog box, you can see how long the test has been running.

To view the unapproved applications that the test logged but did not block

1. In the **System Lockdown name of group** dialog box, click **View Unapproved Applications**.
2. In the **Unapproved Applications** dialog box, review the applications.
This list includes information about the time that the application was run, the computer host name, the client user name, and the executable file name.
3. Determine how you want to handle the unapproved applications.
For allow mode, you can add the names of applications that you want to allow to the list of approved applications. For deny mode, you can remove the names of applications that you want to allow.
4. In the **Unapproved Applications** dialog, click **Reset the Test** if you changed the file fingerprint lists or individual applications and want to run the test again. Otherwise, click **Close**.
5. After you finish testing, you can enable system lockdown.

More information

[Configuring system lockdown](#)

Blocking or allowing devices using Device Control and Application Control

This topic describes how to use the Symantec Endpoint Protection Device Control policy and Application Control policy to allow or block hardware devices on the client computer.

- [How Device Control works](#)
- [Device classes and GUIDs \(class IDs\) and device IDs](#)
- [Using the Symantec DevViewer to find GUIDs and device IDs](#)
- [Best practices for adding GUIDs and device IDs to rules](#)
- [Windows devices that are automatically allowed in Device Control](#)
- [Windows devices that are automatically excluded from Device Control](#)
- [Setting up the Device Control policy](#)

See also: [How Application Control works to block devices](#)

How Device Control works

Symantec Endpoint Protection blocks and allows hardware devices by using Device Control policy rules.

- A Device Control rule that blocks a device disables the device on the Windows Device Manager. A disabled device no longer functions on the Symantec Endpoint Protection client computer.

NOTE

Client users cannot charge devices such as Androids, iPhones, and other types of portable devices when Device Control blocks them using device ID.

- A Device Control rule that allows a device enables the device on the client computer.

The Device Control uses GUIDs (class IDs) or device IDs to identify which hardware device to block or allow.

Symantec Endpoint Protection Manager includes a built-in list of GUIDs and some device IDs in the Hardware Devices list. You can add more GUIDs (for device classes) and device IDs (for unique devices) that operate on the client computer.

Symantec Endpoint Protection Manager

Latest Alerts Refresh Help Log Off

Hardware Devices

Device Name	Platform	Identification
Human Interface Devices (Mice, Joysticks, Gamepads, and Sy...	Windows	Class: {745a17a0-74d3-11d0-b6fe-00a0c90f57da}
USB	Windows	Class: {36fc9e60-c465-11cf-8056-444553540000}
Floppy	Windows	Class: {4d36e969-e325-11ce-bfc1-08002be10318}
1394 FireWire Devices	Windows	Class: {6bdd1fc1-810f-11d0-bec7-08002be2092f}
IDE	Windows	Class: {4d36e96a-e325-11ce-bfc1-08002be10318}
Tape Drives	Windows	Class: {6d807884-7d21-11cf-801c-08002be10318}
CD/DVD Drives	Windows	Class: {4d36e965-e325-11ce-bfc1-08002be10318}
Printing Devices	Windows	Class: {4d36e979-e325-11ce-bfc1-08002be10318}
PCMCIA	Windows	Class: {4d36e977-e325-11ce-bfc1-08002be10318}
Imaging Devices (Scanners, Digital Cameras, etc)	Windows	Class: {6bdd1fc6-810f-11d0-bec7-08002be2092f}
Infrared Devices	Windows	Class: {6bdd1fc5-810f-11d0-bec7-08002be2092f}
Bluetooth Radios	Windows	Class: {e0cbf06c-cd8b-4647-bb8a-263b43f0f974}
SCSI	Windows	Class: {4d36e97b-e325-11ce-bfc1-08002be10318}
Modems	Windows	Class: {4d36e96d-e325-11ce-bfc1-08002be10318}
Smart Card Readers	Windows	Class: {50dd5230-ba8a-11d1-bf5d-0000f805f530}
Ports	Windows	Class: {4d36e978-e325-11ce-bfc1-08002be10318}
Network Adapters	Windows	Class: {4d36e972-e325-11ce-bfc1-08002be10318}

You then add these device IDs to a Device Control policy in a rule that either blocks or allows (excludes) these supported devices.

Application and Device Control Policy

Overview

Application Control

Windows Settings

Device Control

Mac Settings

Device Control

Windows Device Control

Hardware Device Control Lists

Devices a client computer is blocked from accessing, such as USB drives, Bluetooth devices, printers, and serial and parallel ports.

Blocked Devices

Use this pane to manage the list of devices to which you want to block access.

Device Name	Identification
USB Hub	Device: USB\VID_0BDA&PID_5413\B&857A6CF&0&3

Add...

Delete

Devices Excluded From Blocking

Use this pane to manage the list of devices to which you want to allow access.

Device Name	Identification
Infrared Devices	Class: {6bdd1fc5-810f-11d0-bec7-08002be2092f}

After you apply the policy to the client group, Device Control monitors device change messages that the client computer issues. Each time a message occurs (such as when a client user plugs in a USB device), SEP counts all the devices on the computer. SEP checks each device against the rules that apply to the list of device classes that are associated with that device.

Depending on the rule condition type, the Symantec Endpoint Protection client checks the GUID or device ID in two different ways:

- If the Device Control policy specifies a GUID, the Symantec Endpoint Protection client performs a direct string comparison.
- If the Device Control policy specifies a device ID, the Symantec Endpoint Protection client performs a regular expressions match. If a condition is matched, SEP enables or disables the device depending on the rule action. The action to enable or disable the device is much like how a user performs the same operation in Windows Device Manager.

Device classes and GUIDs (class IDs)

Windows organizes hardware devices into a device hierarchy that can have multiple devices per category, called *device classes*. Windows assigns each of these device classes a device *GUID*, which is a unique identifier.

For example:

- Disk Drives - {4d36e967-e325-11ce-bfc1-08002be10318}
- Storage Volumes - {71a27cdd-812a-11d0-bec7-08002be2092f}
- USB devices - {36FC9E60-C465-11CF-8056-444553540000}

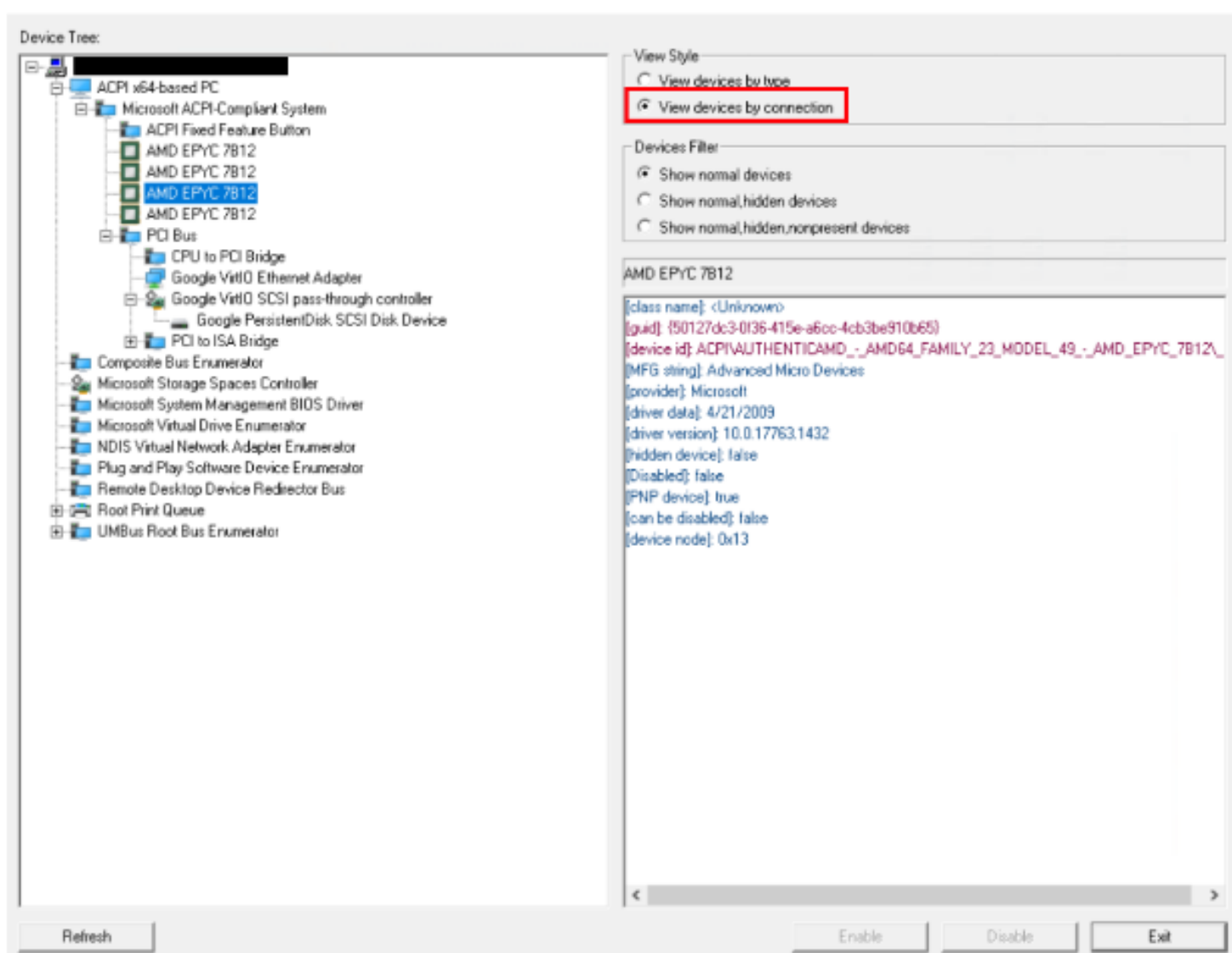
For a list of class IDs, see: [System-Defined Device Setup Classes Available to Vendors](#)

Understanding logical device classes

The Windows device hierarchy includes logical device classes that applies to multiple types of devices. These device classes can include multiple different types of physical device classes, such as the USB device class. Multiple types of classes can potentially cause an unexpected overlap of the policy rules that apply to a specific physical device.

Another example of a logical device class is a *storage volume*, which does not correspond with a specific real physical device type. Windows creates a volume device class after a physical hard disk/USB disk/other storage device is connected to the system and partitions (logical drive letters) are allocated.

The following image of the Symantec DevViewer shows the relationships between different devices. In this case, DevViewer shows the SanDisk Cruzer device hierarchy with both the system-created USB mass storage disk drive and the generic storage volume device classes. When you switch the display from **View devices by connection** to **View devices by type**, these disk and volume devices now appear under the **Disk drives** and **Storage columns** branches.



Understanding the device hierarchy and logical devices helps you to configure the Device Control policy so that it behaves as expected. For example, a rule to block disk drives blocks all physical disks, including internal and external USB disks. Similarly, a rule to block storage volumes blocks all logical partitions without regard to the type of the underlying storage.

When Device Control blocks devices at any parent node in the Windows device hierarchy, it blocks all devices on the child nodes. If a device is allowed at the parent node, all devices are allowed on the child nodes.

Device IDs

A device ID (also known as a device instance ID in Windows) is a specific ID that Windows gives to *each* device. Device IDs generally consist of a type string prefix, such as **IDE\CDROM**, followed by a string that describes the specific device model. For example, two common formats for device IDs include:

- `<class>\<type>&<vendor>&<model>&<revision>\<serial number>`
- `<class>\<type><vendor><model><revision>\<serial number>`

Using the Symantec DevViewer to find GUIDs and device IDs

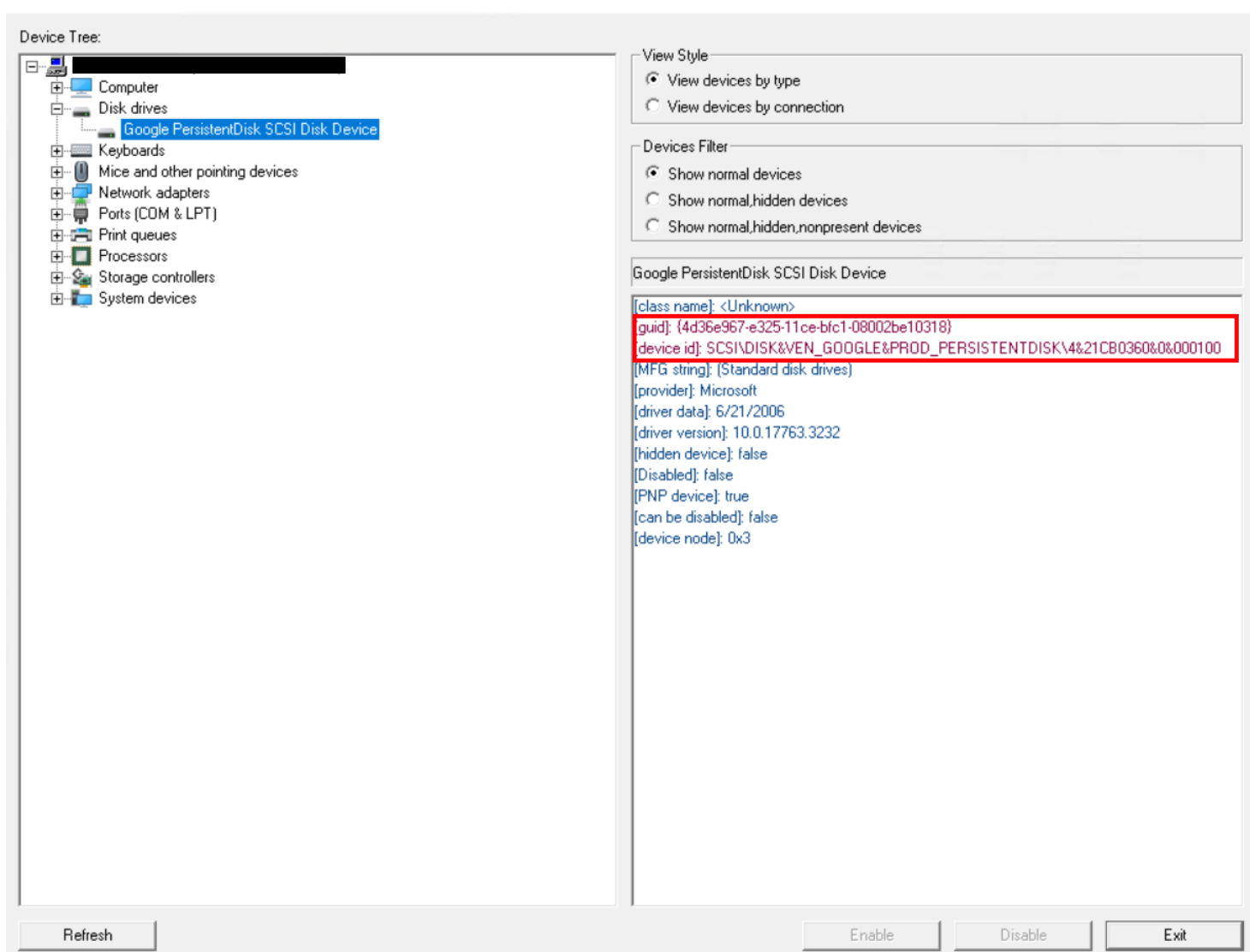
You can use either the Symantec DevViewer or the Windows Device Manager to view the Windows device hierarchy. Both tools show the list of actual hardware devices that are connected to each client computer.

And you can use either tool to find and copy the GUID or device ID for a device and then paste it into the Device Control policy.

However, Symantec recommends that you use DevViewer because the user interface is designed to show all of the necessary device properties more directly.

The DevViewer displays the devices by type or by connection.

The following figure displays the DevViewer interface. In the device properties window, you copy either the class ID [guid] or the device ID [device id] field, and paste it into the Device Control policy. The Device Control policy uses these properties to define the rules that the Symantec Endpoint Protection client matches.



More information

For information on downloading the DevViewer, see: [Use DevViewer to find hardware device IDs for Device Blocking in Endpoint Protection/Endpoint Security](#)

Best practices for adding GUIDs and device IDs to Device Control rules

Use the following information to add a rule to the Device Control policy:

- A *GUID* (device class ID) enables or disables the entire device class. For example, if the USB class GUID is specified in a blocking rule, **all** USB devices are disabled when they connect to USB ports. This device class operates within the hierarchy, since different kinds of physical devices such as cameras, mice, and storage devices are blocked. SEP Device Control can determine the list of device class GUIDs that apply to each physical device.
- A *device ID* enables or disables a specific device, depending on the action of the rule. For example, if you add **IDE \CDROM*** in a blocking rule, all CD/DVD drives that are directly connected to the motherboard are disabled when the Device Control policy is applied to the group.

Usually, Symantec recommends that you use device IDs instead of GUIDs because device IDs:

- Are more specific.
- Can be more effective for blocking or allowing devices because device IDs are made by concatenating a list of data about the particular device. Device IDs are generally in a more readable format.
- Have the lowest potential for unexpected Device Control policy rule behavior, since these rules are the most closely tied to a specific physical device.

Wildcards in device IDs

Symantec supports the * and ? wildcards when adding device IDs to the Hardware Devices list.

- Use * for zero or more of any characters.
- Use ? for a single character of any value.

The following table shows how to use wildcards for device IDs in the Device Control policy.

Table 120: How to use wildcards in device IDs

Type of device	Wildcard
Any USB storage device	USBSTOR*
Any USB Disk	USBSTOR\DISK*
Any USB SanDisk drive	USBSTOR\DISK&VEN_SANDISK*
Any USB SanDisk Micro Cruzer drive	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO*
A specific SanDisk device	USBSTOR \DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0

NOTE

SEP does not support wildcards in GUIDs when you add them to the Device Control policy.

Windows devices that are automatically allowed in Device Control

To protect against policy configurations that render hardware unusable and to save time from adding device classes manually, SEPM includes a list of built-in generic known class IDs. If you create a rule to block these devices, the Symantec Endpoint Protection client ignores the rule and allows the devices anyway.

For example:

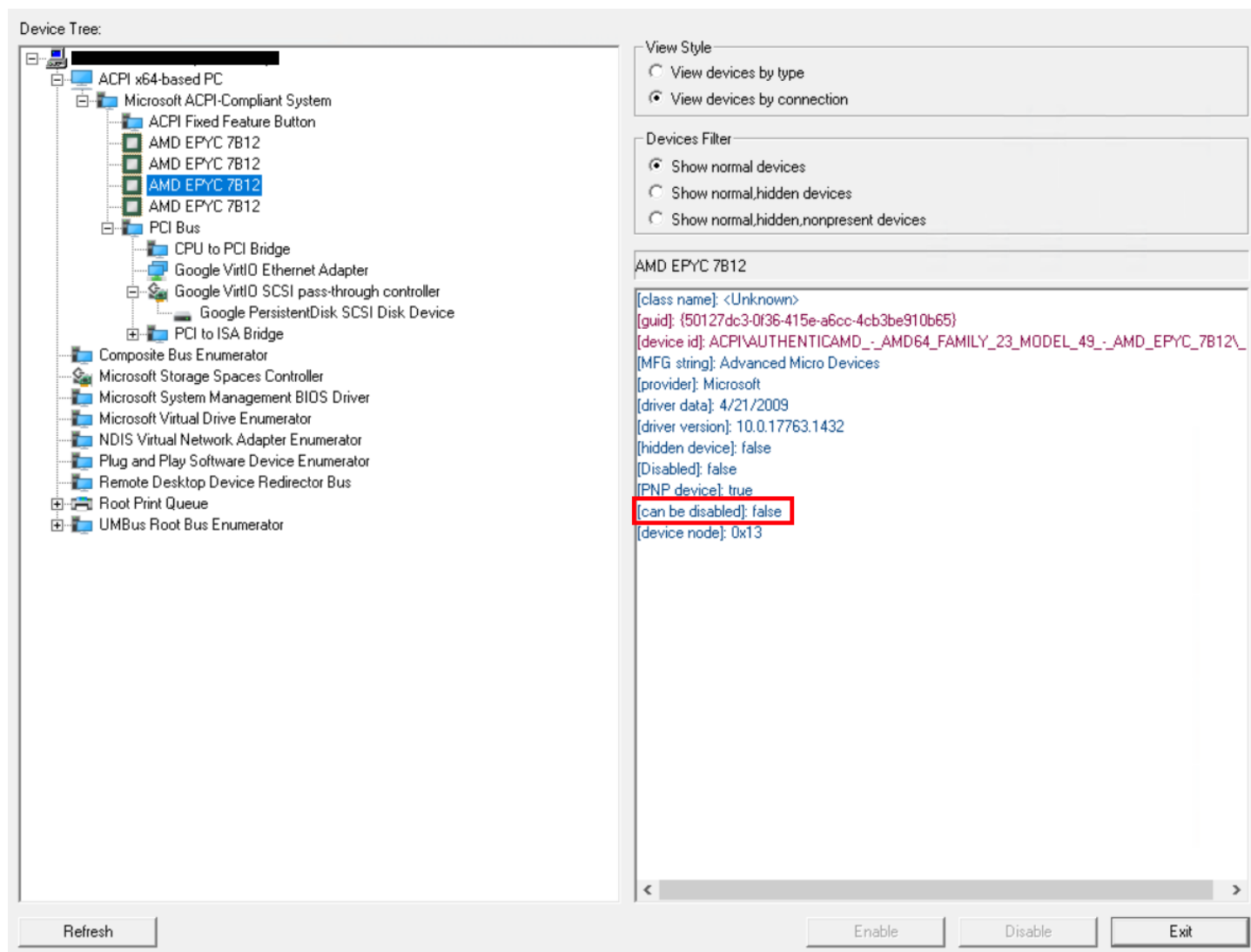
- USB/PCMCIA/FireWire (1394) controllers:
Blocking these devices can cause unexpected behavior, since the controller and any connected devices are affected. Create a policy that targets the devices and device classes that the controller supports.
- Disks and volumes containing the system OS or page file:
Blocking these devices can cause unrecoverable system errors (BSOD). SEP does not disable these devices, but you can block other disks and volumes with the Device Control policy.

Windows devices that are automatically excluded from Device Control

When you create a rule that allows a device, you exclude it from being blocked. You must allow some devices in the following cases:

- Some Windows system critical devices can never be disabled. For example, Windows does not allow Device Control to disable the CPU device.
- You need to block all devices, such as USB storage devices, except for one. The exclusion takes precedence over the block, regardless of what the actual device class entry is.

The following image shows the `[Can be disabled]: false` field in the DevViewer property window. The Symantec Endpoint Protection client checks that this status is `true` before disabling a device. The client does not operate on devices with a `false` status.



To allow a device, you add them to the **Devices Excluded from Blocking** section of the Device Control policy.

Setting up the Device Control policy

You use the DevViewer to find and then copy and paste GUIDs and device IDs into the Hardware Devices list in the Device Control policy.

To set up the Device Control policy

1. [Download](#) and open the DevViewer on the client computer.
2. For each device or device class that you want to block or allow, [copy the GUID or device ID](#) from the DevViewer.
3. Add the GUIDs and device IDs to the Symantec Endpoint Protection Manager Hardware Devices list.
See: [Adding hardware devices to the Hardware Devices list](#)
4. Add the GUIDs and device IDs to the Device Control policy.
See: [Adding Device Control policy rules to allow or block devices on client computers](#)

For information on getting the GUIDs and device IDs from a Mac, see: [Obtaining a device vendor, model, or serial number for Mac devices with DeviceInfo](#)

Adding Device Control policy rules to allow or block devices on client computers

You use an Application and Device Control policy to configure device control. Before you begin, add any devices you need to the **Hardware Devices** list. See:

[Adding a hardware device to the Hardware Devices list](#)

To add device control rules for Windows clients

1. In the console, open an Application and Device Control policy.
2. Click **Device Control**.
3. Do one of the following tasks:
 - To block a device, under **Blocked Devices**, click **Add**.
 - To allow a device, under **Devices Excluded From Blocking**, click **Add**.
4. In the **Device Selection** window, select one or more devices, and then click **OK**.
Make sure that if you block specific ports, then you exclude devices if necessary.

NOTE

Typically, you should never block a keyboard.

5. Check **Notify users when devices are blocked** if you want to notify the user.
6. Click **OK**.

To add device control rules for Mac clients

1. In the console, open an Application and Device Control policy.
2. Under **Mac Settings**, click **Device Control**.
3. Under **Blocked Devices**, click **Add**.
4. In the **Device Selection** window, select a device from the list. You can only add one device at a time.
Fill in the fields at the bottom of the window, if available. If you leave the fields blank, all devices of this type are blocked.
You can also use regular expressions to define device vendor, device model, or serial number. See the Help in the **Mac Device Control** window for more information.
To obtain the serial number, model number, or vendor name from a Mac-connected device, use the DeviceInfo tool from the installation file. You can find this tool and its instructions under `Tools/DeviceInfo`.
5. Click **OK**.
6. Under **Devices Excluded From Blocking**, click **Add**.
7. In the **Device Selection** window, select a device from the list, define the excluded devices, and then click **OK**.
8. Check **Notify users when devices are blocked** if you want to notify the user.
9. Click **OK**.

More information

- [Mac Device Control](#)
- [Managing device control](#)
- [About application control, system lockdown, and device control](#)

Adding hardware devices to the Hardware Devices list

After you obtain a GUID or device ID for a hardware device, you can add the hardware device to the default Hardware Devices list. You can then access this default list from the device control part of the Application and Device Control policy.

For information on GUIDs and device IDs, see: [Blocking or allowing devices using Device Control and Application Control](#)

To add hardware devices to the Hardware Devices list

1. In the console, click **Policies**.
2. Under **Policies**, expand **Policy Components** and click **Hardware Devices**.
3. Under **Tasks**, click **Add a Hardware Device**.
4. Enter the name of the device you want to add.

Both Class IDs and Device IDs are enclosed in curly braces ({ }) by convention. You may need to replace the curly braces with the wildcard character ?.
5. Select either **Class ID** or **Device ID**, and paste the ID that you copied from the Windows Device Manager or the DevViewer tool.
6. You can use wildcard characters to define a set of device IDs. For example, you can use the following string: *IDE \DVDROM*.

For more information, see:
[Obtaining a device vendor or model for Windows computers with DevViewer](#)
7. Click **OK**.

Obtaining a device vendor or model for Windows computers with DevViewer

You can use either the Symantec DevViewer tool or the Microsoft Windows Device Manager to obtain either the class ID (GUID) or the device ID.

After you obtain a device ID, you can modify it in the Device Control policy with a wildcard character to indicate a less specific group of devices.

To obtain a class ID or device ID by using the Symantec DevViewer tool

1. Download DevViewer to the client computer from the Attachments section at:
[Use DevViewer to find hardware device IDs for Device Blocking in Endpoint Protection](#)
2. On the client computer, run `DevViewer.exe`.
3. Expand the **Device Tree** and locate the device for which you want the device ID or the GUID.
For example, expand **Disk drives** and select the device within that category.
4. In the right-hand pane, right-click the [guid] or the [device ID], and then click **Copy GUID** or **Copy Device ID**.
5. Click **Exit**.
6. On the management server, paste the GUID or device ID into the **Policy Components > Hardware Devices** list.

To obtain a device ID from the Microsoft Windows Device Manager

1. In the Control Panel, search for **Device Manager**.
2. In the **Device Manager** dialog box, expand the device class, select the device, and click **Properties**.
3. In the device's **Properties** dialog box, on the **Details** tab, select either **Class GUID** or **Hardware Ids**.
4. Copy the string.
5. Click **OK**.

More information

-
- [Blocking or allowing devices using Device Control and Application Control](#)
 - [Adding Device Control policy rules to allow or block devices on client computers](#)
 - [Adding hardware devices to the Hardware Devices list](#)

Mac Device Control in Endpoint Protection

For each type of policy, you can create a hardware device control list. This list contains a list of blocked devices and a list of devices that are excluded from blocking.

The hardware device control occurs at the file system level. Therefore, the user may still be able to perform volume-level tasks on blocked devices or read-only devices with Disk Utility or Terminal commands. These tasks include erasing, ejecting, or creating a disc image of the blocked device.

The list does not show all of the allowed devices. This list only displays the exceptions to the **Blocked Devices** list.

You should test all device control conditions that you create on a small test group before you apply the policy to all Mac clients. Testing ensures the device control policy blocks devices and excludes devices from blocking as expected.

NOTE

Use caution when blocking by vendor or device ID. Symantec recommends that you do not select non-storage devices that may show up in Finder as devices to be blocked.

You can configure client user interface control settings with **Server Control** or **Mixed Control** mode to prevent users from enabling or disabling device control.

For more information, see:

[Preventing users from disabling protection on client computers](#)

Vendor, model, and serial number fields are not case-sensitive. For each device specified, if you leave the vendor, model, or serial number fields blank, the policy blocks any devices that match the device type. If you do specify values for these fields, type only one value for each of field (e.g., one vendor name in the Vendor field, one model number in the Model field, and one serial number in the Serial No field).

Device control rule conditions give greater precedence to the criteria that are the most specific. For example, the full text string has the greatest precedence, followed next by a partial text string with wildcard, and then by a wildcard only. A blank field acts like a wildcard search, with less weight than the full text string or a partial text string. Similarly, the serial number has a greater precedence than the model name, which takes greater precedence than the vendor name. The full string text for the vendor name takes precedence over the partial string text of the serial number.

The Mac device control conditions are weighted as follows, from greatest weight to least:

- Full string text, serial number
- Full string text, model name
- Full string text, vendor name
- Partial string text with wildcard, serial number
- Partial string text with wildcard, model name
- Partial string text with wildcard, vendor name
- Wildcard only, serial number
- Wildcard only, model name
- Wildcard only, vendor name
- Blank field (nothing defined)

To obtain the serial number, model number, or vendor name from a Mac-connected device, use the DeviceInfo tool from the installation file. You can find this tool and its instructions under `Tools/DeviceInfo`.

The following table lists the device blocking options available for Mac devices.

Table 121: Mac device blocking options

Group or option	Description
Device Name	The name of the device that is blocked or excluded from blocking. You can add or delete devices from this list. The supported device types for Mac are: • Thunderbolt devices • CD/DVD drives • USB devices • FireWire devices • Secure digital (SD) card
Device Vendor	The vendor of the device that is blocked or excluded from blocking. You can block or exclude from blocking all device types except Thunderbolt by specific vendor name. You can use regular expressions to define the vendor name. See: Regular expressions used for device blocking for Mac
Device Model	The model of the device that is blocked or excluded from blocking. You can block or exclude from blocking all device types by specific model. You can use regular expressions to define the model name. See: Regular expressions used for device blocking for Mac
Serial Number	The serial number of the device that is blocked or excluded from blocking. You can only block or exclude from blocking the specific serial numbers of Thunderbolt and USB devices. You can use regular expressions to define the serial number. See: Regular expressions used for device blocking for Mac
Log detected devices	Adds an entry to the device control log whenever Device Control detects a device. This option is enabled by default.
Notify users when devices are blocked or unblocked	Sends a notification to client computers when a blocked device connects or starts up. This option is disabled by default.

The following table describes the regular expressions with which you can define device control criteria.

Table 122: Regular expressions used for device blocking for Mac

Option	Description
. (Dot)	Matches any character but a newline. For example, So*. matches "So", "Soo", "Sooo", "Sobar", "Sooxxx".
\ (Backslash)	Matches the character to follow. The backslash escapes all other meta-characters and itself. When you use backslash in a set, it is considered a regular character. For a binary match, use \x. For example, \xA0 matches binary a0 Hex.
[set], [^Set] (Set)	Matches one of the characters in the set. If the first character in the set is a caret (^), the set attempts to match any characters that are not in the set. The special characters right bracket (]) and hyphen (-) have no special meaning if they appear as the first character in the set. A set can also match a range or characters. For example, S-E would specify a set of characters S through E, inclusive. For example, [a-z] matches any alphabetical character, while [^]\- matches any character except for], \, and -.

Option	Description
* (Star or asterisk)	Any previous regular expression form that concludes with the asterisk (*) matches zero or more matches of that form. For example, Soo* matches "Soo\ ", "Soo\\ ", "Soo\\\ ", and "Soo\\\12".
+ (Plus)	Any previous regular expression form that concludes with the plus (+) matches one or more matches of that form. For example, Soo\+ matches "Soo\ ", "Soo\\ ", and "Soo\\\ ", but it does not match "Soo\\\12".

Obtaining a device vendor, model, or serial number for Mac devices with DeviceInfo

You can use the DeviceInfo tool to obtain the device vendor, model, or serial number for a specific device on the Mac client to use in Device Control policies.

NOTE

This tool only works to identify this information for mounted devices. This tool does not recognize non-mounted devices.

To obtain a device vendor, model, or serial number for Mac devices with DeviceInfo

1. In the installation file, locate the \Tools\DeviceInfo folder, and then copy this folder to the desktop of the Mac client computer.
2. On the Mac client computer, ensure the device for which you want to obtain information is connected, and then open the Terminal application.
3. To navigate to the tool's folder, type the following command:

```
cd ~/Desktop/DeviceInfo/
```

4. To obtain the device's information, enter the following command:

```
./DeviceInfo
```

5. Make note of the relevant information from the results, for use in your device control policy for Mac.

How Application Control works to block devices

Application Control blocks devices more granularly by blocking or allowing read, write, or execute commands on a device. Application Control also controls what applications can be used.

For example, the policy can block any program that runs from a USB drive and that could change the registry or modify files on the host computer.

With Application Control, you can use device IDs but not GUIDs.

You can use device IDs in the following rule conditions:

- Application rule process
- Launch Process Attempts
- Terminate Process Attempts
- File and Folder Access Attempts
- Load DLL Attempts

Application Control only blocks a device that is the last node in the device hierarchy, unless the last node is a **Generic volume** or **Storage volume**. In these two cases, the device that is the parent node of the last node is blocked.

Most device IDs that Application Control supports have one of these types:

Type of device	Example
USBSTOR	USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0
FCD	FDC\GENERIC_FLOPPY_DRIVE\4&371082C9&0&0
DE	IDE\DISKHTS541060G9SA00_____MB3IC60H\4&14AA9DA8&0&0.0.0
SCSI	SCSI\DISK&VEN_WDC_WD50&PROD_00KS-00MNB0&REV_700.14&1291CDED&0&000

NOTE

Application Control can only block devices that Windows sees as disk drives and that have drive letters that are associated with them. Devices that do not add drive letters (such as an iPhone or iPad) must be blocked using Device Control. See:

[Block USB devices, excluding the mouse and keyboard, in the Symantec Endpoint Protection Manager.](#)

For more information on GUIDs and device IDs, see: [Blocking or allowing devices using Device Control and Application Control](#)

Applying exceptions to scans in Symantec Endpoint Protection

You can manage exceptions for Symantec Endpoint Protection in the Symantec Endpoint Protection Manager console.

Table 123: Managing exceptions

Task	Description
Learn about exceptions	You use exceptions to exclude items from being scanned on your client computers.
Review the types of files and folders that Symantec Endpoint Protection automatically excludes from scans	Symantec Endpoint Protection automatically creates exceptions, or exclusions, for some third-party applications and some Symantec products. You can also configure individual scans to scan only certain extensions and skip any other extensions. See: About the files and folders that Symantec Endpoint Protection excludes from virus and spyware scans
Create exceptions for scans	You add exceptions in an Exceptions policy directly. Or you can add exceptions from log events on the Monitors page. See: Creating exceptions for Virus and Spyware scans Creating exceptions from log events
Restricting the types of exceptions that users can configure on client computers (Windows only)	By default, users on client computers have limited configuration rights for exceptions. You can restrict users further so that they cannot create exceptions for virus and spyware scans or for behavioral analysis. Users can never force an application detection and they never have permission to create Tamper Protection exceptions. Exceptions that client users create (called <i>user-defined exceptions</i>), do not get uploaded to the management server. Users also cannot create a file exception for application control. See: Restricting the types of exceptions that users can configure on client computers
Check the logs for detections for which you might want to create exceptions	After Symantec Endpoint Protection makes a detection, you can create an exception for the detection from the log event. For example, you might want to create an exception for a file that scans detect but that your users request to download. See: Creating exceptions from log events

Task	Description
Create exceptions for intrusion prevention signatures	You can specify exceptions for intrusion prevention. You can also set up a list of excluded hosts for intrusion prevention. Intrusion prevention exceptions are configured in an Intrusion Prevention policy. See: Creating exceptions for IPS signatures

Which Windows exceptions do I use for what type of scan?

The following table lists which exception types are used in the Exceptions policy for which types of scans.

Table 124: Exception names

Symantec Endpoint Protection Manager	Client restrictions (on Symantec Endpoint Protection Manager)*	Windows client	What is exception used for?
Application	Application Exception	Application Exception	• Auto-Protect • Manual scans • Scheduled scans • Download Insight • Behavioral analysis
Application to Monitor	Not available	Not available	Application Control
Certificate	Not available	Not available	• Auto-Protect • Manual scans • Scheduled scans • Download Insight • Behavioral analysis
DNS or Host File Change	DNS or Host File Change Exception	DNS or Host File Change Exception > Application	Behavioral analysis
Extensions	Extensions Exception	Security Risk Exception > Extensions	• Auto-Protect • Manual scans • Scheduled scans
File	File Exception	Security Risk Exception > File	• Auto-Protect • Manual scans • Scheduled scans • Behavioral analysis • Application Control
File Access	File Access		Application Control
Folder	Folder Exception: • Security risk Exception • SONAR Exception	Security Risk Exception > Folder SONAR Exception	• Auto-Protect • Manual scans • Scheduled scans • Behavioral analysis • Application Control
Known Risks	Known risks Exception	Security Risk Exception > Known Risks	• Auto-Protect • Manual scans • Scheduled scans • Behavioral analysis
Trusted Web Domain	Trusted web domain Exception	Security Risk Exception > Web Domain	Download Insight

Symantec Endpoint Protection Manager	Client restrictions (on Symantec Endpoint Protection Manager)*	Windows client	What is exception used for?
Tamper Protection Exception	Not available	Not available	Applications that Tamper Protection protects

*Client restrictions are the exceptions that you can display or hide on the client for the client user to add. Exceptions that you add in the cloud console are unavailable in Symantec Endpoint Protection Manager to enable or disable on the client.

See: [Restricting the types of exceptions that users can configure on client computers](#)

Creating exceptions for Virus and Spyware scans

You can create different types of exceptions for Symantec Endpoint Protection.

Any exception that you create takes precedence over any exception that a user might define. On client computers, users cannot view the exceptions that you create. A user can view only the exceptions that the user creates.

Exceptions for virus and spyware scans also apply to Download Insight.

Table 125: Creating exceptions for Symantec Endpoint Protection

Task	Description
Exclude a file from virus and spyware scans	Supported on Windows and Mac clients. Excludes a file by name from virus and spyware scans, behavioral analysis, or application control on Windows clients. For more information, see: Excluding a file or a folder from scans
Exclude a folder from virus and spyware scans	Supported on Windows, Mac, and Linux clients. Excludes a folder from virus and spyware scans, behavioral analysis, or all scans on Windows clients. On Windows and Linux clients, you can choose to limit an exception for virus and spyware scans to Auto-Protect or scheduled and on-demand scans only. If you run an application that writes many temp files to a folder, you might want to exclude the folder from Auto-Protect. Auto-Protect scans files as they are written so you can increase computer performance by limiting the exception to scheduled and on-demand scans. You might want to exclude the folders that are not often used or that contain archived or packed files from scheduled and on-demand scans. For example, scheduled or on-demand scans of deeply archived files that are not often used might decrease computer performance. Auto-Protect still protects the folder by scanning only when any files are accessed or written to the folder. For more information, see: Excluding a file or a folder from scans
Exclude a known risk from virus and spyware scans	Supported on Windows clients. Excludes a known risk from virus and spyware scans. The scans ignore the risk, but you can configure the exception so that the scans log the detection. In either case, the client software does not notify users when it detects the specified risks. If a user configures custom actions for a known risk that you configure to ignore, Symantec Endpoint Protection ignores the custom actions. Security risk exceptions do not apply to behavioral analysis. For more information, see: Excluding known risks from virus and spyware scans on Windows clients

Task	Description
Exclude file extensions from virus and spyware scans	Supported on Windows and Linux clients. Excludes any files with the specified extensions from virus and spyware scans. Extension exceptions do not apply to behavioral analysis or to Power Eraser. For more information, see: Excluding file extensions from virus and spyware scans on Windows clients and Linux clients
Monitor an application to create an exception for the application	Supported on Windows clients. Use the Application to monitor exception to monitor a particular application. When Symantec Endpoint Protection learns the application, you can create an exception to specify how Symantec Endpoint Protection handles the application. If you disable application learning, the Application to monitor exception forces application learning for the application that you specify. For more information, see: Creating an application exception
Specify how virus and spyware scans handle monitored applications	Supported on Windows clients. Use an application exception to specify an action for Symantec Endpoint Protection to apply to a monitored application. The type of action determines whether Symantec Endpoint Protection applies the action when it detects the application or when the application runs. Symantec Endpoint Protection applies the Terminate, Quarantine, or Remove action to an application when it launches or runs. It applies the Log only or Ignore action when it detects the application. Unlike a file name exception, an application exception is a hash-based exception. Different files can have the same name, but a file hash uniquely identifies an application. The application exception is a SHA-2 hash-based exception. Applications for which you can create exceptions appear in the Exceptions dialog after Symantec Endpoint Protection learns the application. You can request that Symantec Endpoint Protection monitors a specific application to learn. For more information, see: • Creating an application exception • Enabling application learning
Exclude a web domain from virus and spyware scans	Supported on Windows clients. Download Insight scans the files that users try to download from websites and other portals. Download Insight runs as part of a virus and spyware scan. You can configure an exception for a specific web domain that you know is safe. Download Insight must be enabled for the exception to have any effect. Note: If your client computers use a proxy with authentication, you must specify trusted web domain exceptions for Symantec URLs. The exceptions let your client computers communicate with Symantec Insight and other important Symantec sites. See the following articles: • How to test connectivity to Insight and Symantec licensing servers • Required exclusions for proxy servers to allow Symantec Endpoint Protection to connect to Symantec reputation and licensing servers For more information, see: Excluding a trusted web domain from scans on Windows clients

Task	Description
Create file exceptions for Tamper Protection	Supported on Windows clients. Tamper Protection protects client computers from the processes that tamper with Symantec processes and internal objects. When Tamper Protection detects a process that might modify the Symantec configuration settings or Windows registry values, it blocks the process. Some third-party applications inadvertently try to modify Symantec processes or settings. You might need to allow a safe application to modify Symantec settings. You might want to stop Tamper Protection for certain areas of the registry or certain files on the client computer. In some cases, Tamper Protection might block a screen reader or some other assistive technology application. You can create a file exception so that the application can run on client computers. Folder exceptions are not supported for Tamper Protection. For more information, see: Creating a Tamper Protection exception on Windows clients
Allow applications to make DNS or host file changes	Supported on Windows clients. You can create an exception for an application to make a DNS or host file change. Behavioral analysis typically prevents system changes like DNS or host file changes. You might need to make an exception for a VPN application, for example. For more information, see: Creating an exception for an application that makes a DNS or host file change
Exclude a certificate	Supported on Windows clients. You can exclude a certificate from scans. Excluding a certificate prevents it from being flagged as suspicious. A Download Insight scan can flag a self-signed certificate on an internal tool as suspicious, for example. For more information, see: Excluding a certificate from scans on Windows clients

More information

- [Managing exceptions in Symantec Endpoint Protection](#)
- [Creating exceptions from log events](#)

Excluding a file or a folder from scans

You add exceptions for files or folders individually. If you want to create exceptions for more than one file, repeat the procedure.

You can configure file or folder exceptions on both Windows and Mac clients and file exceptions on Linux clients.

To exclude a file from scans on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Under **Exceptions**, click **Add > Windows Exceptions > File**.
3. In the **Prefix variable** drop-down box, select a common folder.
Select **[NONE]** to enter the absolute path and file name.
When you select a prefix, the exception can be used on different Windows operating systems.
4. In the **File** text box, type the name of the file.
If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

NOTE

Paths must be denoted by using a backward slash.

NOTE

The Windows client does not support the use of UNC paths in exceptions. Auto-Protect ignores these exceptions. On-demand scans and scheduled scans, and other protection technologies do not exclude those

locations reliably. Instead, you should map UNC locations to a drive in Windows and should create mapped drive letter exceptions for the best performance and reliability.

- Under **Specify the types of scans that will exclude this file**, select the type of scan (**Security Risk**, **SONAR**, or **Application control**).

You must select at least one type.

- For security risk scans, under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.

See the help for information about why you might want to limit the exception to a specific type of security risk scan.

- Click **OK**.

To exclude a folder from scans on Windows clients

- on the **Exceptions Policy** page, click **Exceptions**.
- Under **Exceptions**, click **Add > Windows Exceptions > Folder**.
- In the **Prefix variable** drop-down box, select a common folder.

Select **[NONE]** to enter the absolute path and file name.

When you select a prefix, the exception can be used on different Windows operating systems.

- In the **Folder** text box, type the name of the folder.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

NOTE

Paths must be denoted by using a backward slash.

- Under **Specify the type of scan that excludes this folder**, select the type of scan (**Security Risk**, **SONAR**, **Application control**, or **All**).

You must select at least one type.

- For security risk scans, under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.

See the help for information about why you might want to limit the exception to a specific type of security risk scan.

- Click **OK**.

To exclude a file or folder from scans on Mac clients

- On the **Exceptions Policy** page, click **Exceptions**.
- Under **Exceptions**, click **Add > Mac Exceptions > Security Risk Exceptions for File or Folder**.
- Under **Security Risk File or Folder Exception**, in the **Prefix variable** drop-down box, select a common folder.

Select **[NONE]** to enter the absolute path and file name.

- In the **File or Folder** text box, type the name of the file or folder.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

NOTE

Folder paths must be denoted by using a forward slash.

- Click **OK**.

To exclude a folder from scans on Linux clients

- On the **Exceptions Policy** page, click **Exceptions**.
- Under **Exceptions**, click **Add > Linux Exceptions**.
- Click **Folder**.
- In the **Add Folder Exception** dialog box, you can choose a prefix variable, type a folder name, and either include subfolders or not.

As of 14.3 RU1, the option **Also exclude subfolders** is not supported in Symantec Agent for Linux and all subdirectories are always excluded from the scans.

If you select a prefix variable, the path should be relative to the prefix. If you select **[NONE]**, type the full path name.

NOTE

Folder paths must be denoted by using a forward slash.

5. Specify the type of security risk scan. Select **Auto-Protect**, **Scheduled and on-demand**, or **All scans**, and then click **OK**.

More information

- [Creating exceptions for Virus and Spyware scans](#)
- [Excluding file extensions from virus and spyware scans on Windows clients and Linux clients](#)

Excluding known risks from virus and spyware scans on Windows clients

The security risks that the client software detects appear in the **Known Security Risk Exceptions** dialog box.

The known security risks list includes information about the severity of the risk.

To exclude known risks from virus and spyware scans on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Under **Exceptions**, click **Add > Windows Exceptions > Known Risks**.
3. In the **Add Known Security Risk Exceptions** dialog box, select one or more security risks that you want to exclude from virus and spyware scans.
4. Check **Log when the security risk is detected** if you want to log the detection.
If you do not check this option, the client ignores the risk when it detects the selected risks. The client therefore does not log the detection.
5. Click **OK**.
6. If you are finished with the configuration for this policy, click **OK**.

More information

[Creating exceptions for Virus and Spyware scans](#)

Excluding file extensions from virus and spyware scans on Windows clients and Linux clients

You can add multiple file extensions to an exception. After you create the exception, you cannot create another extensions exception for the same policy. You must edit the existing exception.

You can add only one extension at a time. If you enter multiple extension names in the **Add** text box, the policy treats the entry as a single extension name.

For more information, see:

[Creating exceptions for Virus and Spyware scans](#)

To exclude file extensions from virus and spyware scans on Windows clients and Linux clients

-
1. On the **Exceptions Policy** page, click **Exceptions**.
 2. Under **Exceptions**, click **Add > Windows Exceptions > Extensions** or **Add > Linux Exceptions > Extensions**.
 3. In the text box, type the extension that you want to exclude, and then click **Add**.
 4. Under **Specify the type of security risk scan**, select **Auto-Protect**, **Scheduled and on-demand**, or **All Scans**.
 5. Add any other extensions to the exception.
 6. Click **OK**.

More information

[Excluding a file or a folder from scans](#)

Creating an application exception

You can prevent the Symantec Endpoint Protection (SEP) client from scanning or detecting an application that you know is safe.

You can monitor a particular application so that you can create an exception for how Symantec Endpoint Protection handles the application. After Symantec Endpoint Protection learns the application and the management console receives the event, the application appears in the application list in the Application Exception dialog. The application list appears empty if the client computers in your network have not yet learned any applications.

The applications list includes the applications that you monitor as well as the files that your users download. Symantec Endpoint Protection applies the action when either Symantec Endpoint Protection detects the application or the application runs.

The applications also appear in the list for **DNS and Host File Change Exception**.

To force the client to learn an application

You can enable application learning in the following ways:

1. If you know the name of the application you would like to learn, configure the SEP clients to monitor that application and learn its fingerprint.
If you disable application learning, the **Application to Monitor** exception forces application learning for the specified application.
See: [Application to Monitor](#)
2. If you do not know the name of the application and want to monitor all applications on a client, configure the SEP clients to monitor all applications and learn their fingerprints. Perform application learning temporarily and on a small subset of clients. Otherwise, this list can get large quickly.
See: [Enabling application learning](#)

To create an application exception

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > Application**.
3. In the **View** drop-down list, select **All**, **Watched Applications**, or **User-allowed Applications**.
4. Select the applications for which you want to create an exception.
5. In the **Specify the action to take on this application** drop-down box, select **Ignore** or **Log only**.
 - The **Ignore** and **Log only** actions exclude the application from detection and allow it to run.
 - The **Terminate**, **Quarantine**, and **Remove** actions apply when the application launches. Use these actions for an application that is bad or malicious.
6. Click **OK**.

The application also appears in the relevant log, and you can create an exception from the log.

To create an application exception with the file fingerprint (SHA256 hash)

If you know the fingerprint (SHA256 hash) of the application, enter it directly or enable application monitoring to allow the SEP client to learn the applications on the client computer and then create an exception from the learned list.

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > Application**.
3. Click **Add an Application by Fingerprint**
4. Enter the application fingerprint and application name (optional).
5. In the **Specify the action to take on this application**, select **Ignore** or **Log only**.
6. Click **OK**.

More information

- To find applications that the client computers run, see: [Searching for information about the learned applications that the computers run](#)
- In 14.3 RU3 and later, application exceptions are only supported in Windows. If you want application exceptions to be supported in other operating systems such macOS and Linux, send an [enhancement request](#).
- Auto-Protect process exclusions are not configured in the Exceptions Policy. To configure Auto-Protect process exclusions, see: [Preventing SEP from scanning files accessed by a trusted process](#).

Excluding a trusted web domain from scans on Windows clients

You can exclude a web domain from virus and spyware scans and from behavioral analysis. When you exclude a trusted web domain, any file that the user downloads from any location within that domain is always allowed. However, Auto-Protect and other defined scans still scan the file.

By default, Download Insight excludes the websites that appear on the **Internet Trusted Sites** list through **Internet Explorer > Tools > Internet Options > Security**. You can configure this setting from the Download Insight settings in the **Virus and Spyware Protection** policy.

If Download Insight or Auto-Protect is disabled, trusted web domain exceptions are also disabled.

NOTE

You should use caution when you configure exceptions. Every exception that you create lowers the security profile of the computer. Consider submitting any suspected false positives for examination rather than opening a permanent scan exclusion. Always use the multiple layers of protection that Symantec Endpoint Protection provides. See:

[Report a Suspected Erroneous Detection \(False Positive\)](#)

Supported web domain exceptions

Follow these guidelines when you create a web domain exception:

-
- You must enter a single domain as a URL or an IP address when you specify a trusted web domain exception. You can specify only one domain at a time.
 - Port numbers are not supported.
 - When you specify a URL, the exception uses only the domain name portion of a URL. You can prepend the URL with either HTTP or HTTPS (case-insensitive), but the exception applies to both protocols.
 - When you specify an IP address, the exception applies to both the specified IP address and its corresponding host name. If a user navigates to a location through its URL, Symantec Endpoint Protection resolves the host name to the IP address and applies the exception. You can prepend the IP address only with HTTP (case-insensitive).
 - Both Download Insight and behavioral analysis exclude the domain regardless of whether a user navigates to the domain through HTTP or HTTPS.
 - For an FTP location, you must specify an IP address. FTP URLs are not supported.
 - The wildcard * is supported for use with exceptions for trusted web domains.
 - URL reputation in the Intrusion Prevention policy allows any websites that you specify as a Trusted Web Domain Exception.

To exclude a trusted web domain from scans on Windows clients

1. On the **Exceptions Policy** page, click **Add > Windows Exceptions > Trusted Web Domain**.
2. In the **Add Trusted Web Domain Exception** dialog box, enter the domain name or IP address that you want to exclude.
3. Click **OK**.
4. Repeat the procedure to add more web domain exceptions.

More information

[Creating exceptions for Virus and Spyware scans](#)

Creating a Tamper Protection exception on Windows clients

You can create file exceptions for Tamper Protection. You might want to create a Tamper Protection exception if Tamper Protection interferes with a known safe application on your client computers. For example, Tamper Protection might block an assistive technology application, such as a screen reader.

You need to know the name of the file that is associated with the assistive technology application. Then you can create an exception to allow the application to run.

NOTE

Tamper Protection does not support folder exceptions.

14.2 RU1 and later includes support for the **[User Profile]** and **[System]** prefix variables.

To create Tamper Protection exception on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > Tamper Protection Exception**.
3. In the **Add Tamper Protection Exception** dialog box, in the **Prefix variable** drop-down box, select a common folder.
When you select a prefix, the exception can be used on different Windows operating systems.
Select **[NONE]** if you want to enter the absolute path and file name.
4. In the **File** text box, type the name of the file.
If you selected a prefix, the path should be relative to the prefix. If you selected **[NONE]** for the prefix, type the full path name.

You must specify a file name. Tamper Protection does not support folder exceptions. If you enter a folder name, Tamper Protection does not exclude all the files in a folder with that name. It only excludes a file with that specified name.

5. Click **OK**.

More information

[Creating exceptions for Virus and Spyware scans](#)

Creating an exception for an application that makes a DNS or host file change

You can create an exception for a specific application that makes a DNS or host file change. SONAR might prevent system changes like DNS or host file changes. You might need to make an exception for a VPN application, for example.

You can monitor a particular application so that you can create a DNS or host file change exception. After Symantec Endpoint Protection learns the application and the management console receives the event, the application appears in the application list. The application list appears empty if the client computers in your network have not yet learned any applications.

Use the SONAR settings to control how SONAR detects DNS or host file changes globally.

To create an exception for an application that makes a DNS or host file change

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Click **Add > Windows Exceptions > DNS or Host File Change Exception**.
3. Select the applications for which you want to create an exception.
4. In the **Action** drop-down box, select **Ignore**, **Log only**, **Prompt**, or **Block**.

The actions apply when scans detect the application making a DNS or host file change.

5. Click **OK**.

More information

- [Creating exceptions for Virus and Spyware scans](#)
- [Creating an application exception](#)
- [Adjusting SONAR settings on your client computers](#)

Excluding a certificate from scans on Windows clients

You can add exceptions for certificates individually to prevent the files that it signs from being scanned and detected as suspicious. For example, a tool that your company developed internally may use a self-signed certificate. Excluding this certificate from scans prevents Auto-Protect, Download Insight, SONAR, or other scans from detecting the files that it signs as suspicious.

The certificate exclusion supports the X.509 and base64 certificate types only. When you add a certificate exception, you need a copy of the public certificate in a DER or base64 encoded file (.cer).

Certificate exclusions are not supported for the following items:

- Memory Exploit Mitigation
- Proactive Threat Protection system change events
- Tamper Protection
- Certificate-signed files within a compressed file

The excluded certificate does not have to be installed in the certificate store on the client computer in order for the exclusion to work. In the case of a conflict between a certificate exception and a deny list rule, the deny list rule takes precedence.

You can only add a certificate exception through the Symantec Endpoint Protection Manager policy, not through the Symantec Endpoint Protection client interface settings.

NOTE

You can only add a certificate exception in Symantec Endpoint Protection Manager if it is unenrolled from the cloud console. If Symantec Endpoint Protection Manager is enrolled, use the cloud console to add or manage a certificate exception.

To exclude a certificate from scans on Windows clients

1. On the **Exceptions Policy** page, click **Exceptions**.
2. Under **Exceptions**, click **Add > Windows Exceptions > Certificate**.
If Symantec Endpoint Protection Manager is enrolled in the cloud console, this option does not appear. Instead, add certificate exceptions in the cloud console.
3. Under **Certificate File**, click **Browse** to navigate to the certificate that you want to exclude, and then click **OK**.
4. Confirm that the values under **Certificate Information** are correct for the certificate that you want to exclude, and then click **OK**.

To create exceptions for more than one certificate, repeat the procedure.

More information

[Creating exceptions for Virus and Spyware scans](#)

Restricting the types of exceptions that users can configure on client computers

You can users on client computers from creating exceptions for scans, called user-defined exceptions. By default, users are permitted to configure exceptions. If a user already created an exception before you turned off this ability, the exceptions still exist.

Users on client computers can never create exceptions for Tamper Protection, regardless of the restriction settings.

Users also cannot create file exceptions for application control.

NOTE

Exceptions that client users create (called *user-defined exceptions*), do not get uploaded to the management server.

To restrict the types of exceptions that users can configure on client computers

1. On the **Exceptions Policy** page, click **Client Restrictions**.
2. Under **Client Restrictions**, uncheck any exception that you do not want users on client computers to configure.
3. If you are finished with the configuration for this policy, click **OK**.

More information

[Managing exceptions in Symantec Endpoint Protection](#)

Creating exceptions from log events

You can create exceptions from log events for virus and spyware scans, behavioral analysis, application control, and Tamper Protection.

NOTE

You cannot create exceptions from log events for early launch anti-malware detections.

For Linux Agents, you can create exceptions for folders and extensions but not for files.

Table 126: Exceptions and log types

Exception Type	Log Type
File	Risk log
Folder	Risk log SONAR log
Known risk	Risk log
Extension	Risk log
Application	Risk log SONAR log
Trusted Web domain	Risk log SONAR log
Tamper Protection	Application Control log
DNS or host file change	SONAR log

Symantec Endpoint Protection must have already detected the item for which you want to create an exception. When you use a log event to create an exception, you specify the Exceptions policy that should include the exception.

To create exceptions from log events

1. On the **Monitors** tab, click the **Logs** tab.
2. In the **Log type** drop-down list, select the Risk log, SONAR log, or Application and Device Control log.
3. If you selected Application and Device Control, select **Application Control** from the **Log content** list.
4. Click **View Log**.
5. Next to **Time range**, select the time interval to filter the log.
6. Select the entry or entries for which you want to create an exception.
7. Next to **Action**, select the type of exception that you want to create.

The exception type that you select must be valid for the item or items that you selected.

8. Click **Apply** or **Start**.
9. In the dialog box, remove any items that you do not want to include in the exception.
10. For security risks, check **Log when the security risk is detected** if you want Symantec Endpoint Protection to log the detection.
11. Select all of the Exceptions policies that should use the exception.
12. Click **OK**.

More information

- [Monitoring the Symantec Endpoint Protection clients](#)
- [Managing exceptions in Symantec Endpoint Protection](#)
- [Creating exceptions for Virus and Spyware scans](#)

Controlling Internet access with Web and Cloud Access Protection

The Web and Cloud Access Protection policy integrates Symantec Cloud Secure Web Gateway (Cloud SWG) functionality into Symantec Endpoint Protection. Web and Cloud Access Protection policy automatically redirects all Internet traffic on the client to the Cloud SWG, where the traffic is allowed or blocked based on the Cloud SWG policies.

To use this feature in Symantec Endpoint Protection Manager (SEPM), you must have a valid Cloud SWG subscription. Contact your account representative for a subscription.

You should perform thorough testing with your applications against your Cloud SWG policies.

NOTE

The Symantec Web Security Service (WSS) was renamed to the Symantec Cloud Secure Web Gateway (Cloud SWG) in 2022.

Configuring Web and Cloud Access Protection with the tunnel method

In 14.3 RU8 and later, the tunnel method is the only way to integrate with Cloud SWG. The tunnel method runs on Windows clients only.

Table 127: Configuring the tunnel method

Steps	Description
Step 1: Configure the Web and Cloud Access Protection policy for the tunnel method in Symantec Endpoint Protection Manager (SEPM).	- In the SEPM, in the Web and Cloud Access Protection policy, make sure that the Redirection method is set to Tunnel. See "Step 3—Configure Web and Access Cloud Protection in the SEP Manager" in the following topic: SEP Web and Cloud Access Protection—Tunnel Mode - Choose an Identify Traffic option (14.3 RU5 and later). The following diagram displays a decision tree to help you choose which traffic identification method to use. <pre> graph TD Q1{Is this a true multi-user windows environment (Windows 10 multi-session, VDI)?} Q2{Is a tunnel required prior to console user availability (RDP, Azure AD forgot password)?} Q3{Do you authenticate your users to WSS using SAML?} A1([Use the Based on the running process option]) A2([Use the Based on the console user option]) A3([Use the Based on the running process option]) A4([Use the Using WSS SAML authentication option]) Q1 -- Yes --> A1 Q1 -- No --> Q2 Q2 -- Yes --> Q3 Q2 -- No --> A2 Q3 -- Yes --> A4 Q3 -- No --> A3 </pre> For a description of each traffic identification method, see: Web and Cloud Access Protection Settings (Optional) To use the SAML authentication method on the Symantec Endpoint Protection client, first enable SAML authentication on the Cloud SWG portal. See: About SAML Authentication and Cloud SWG SAML Support for WSS Agent - Generate and paste the integration token that you obtained from the Cloud SWG. You obtain the token from the Cloud SWG portal by navigating to Connectivity > WSS Agent. Agent Token: - Keep the policy unlocked. - Assign the Web and Cloud Access Protection policy to the test group.
Step 2: Check that Web and Cloud Access Protection policy is enabled on the client.	While you test the SEP client, make sure that the Web and Cloud Access Protection policy is enabled and connected to Cloud SWG. Verifying that the Web and Cloud Access Protection tunnel method is enabled and connected on the Windows client
Step 3: Configure and test Cloud SWG policies.	To test Web and Cloud Access Protection, you first set up or modify the Cloud SWG policies in a lab environment. You then run the various test scenarios against the Cloud SWG policy, which often involves comparing the client's compliance against a Cloud SWG policy.
Step 4: Lock the Web and Cloud Access Protection policy.	After you are sure that the Cloud SWG policies work the way you expect them to on the Symantec Endpoint Protection client, lock the policy. The client computer is then protected and that the user cannot disconnect the client from the Cloud SWG. To lock Web and Cloud Access Protection, lock the padlock in the SEPM Web and Cloud Access Protection policy.

NOTE

In 14.3 RU4, the default traffic identification method is **Based on the running process**. In 14.3 RU5 and later, the default identification method is **Based on the console user**. If you upgrade to 14.3 RU5 or later and the Web and Cloud Access Protection policy is already applied to client groups, the traffic identification method remains as **Based on the running process**.

To use a Host Integrity policy template to install the WebView2 application on the client computers, or to migrate a standalone WSS Agent to a SEP client that includes Web and Cloud Access Protection, see: [Troubleshooting Web and Cloud Access Protection](#)

Configuring Web and Cloud Access Protection with the PAC file method (14.0.1 MP1 to 14.3 RU7)

NOTE

The PAC file method was removed in 14.3 RU8. To use Web and Cloud Access Protection on Windows clients, you must use the tunnel method. For Mac clients, you must use either a Symantec Endpoint Protection Manager or a Mac client version 14.3 RU4 through 14.3 RU7. See:

[Migrating Web and Cloud Access Protection from the PAC file redirection method to the tunnel method](#)

The Cloud SWG administrator provides the Proxy Auto Configuration (PAC) file URL or the integration token from the Cloud SWG portal. You then update the Web and Cloud Access Protection policy with the PAC file or integration token, and assign the Web and Cloud Access Protection policy to a group. See:

[SEP Web and Cloud Access Protection—Explicit Mode](#)

Sending notifications when content is blocked using the Block Notification Service (Optional)

If your Cloud SWG account is integrated with CloudSOC, you can use the Block Notification Service (BNS). The BNS provides out-of-band notifications to SEP clients when content is blocked by CloudSOC gatelet (CASB/DLP) policies.

[WSS Agent Block Notification Service](#)

Reporting

- Configuration changes to the Web and Cloud Access Protection policy appear in the Symantec Endpoint Protection Manager Audit log.
- Events for the tunnel method appear in the client Web and Cloud Access Protection log. These events get uploaded to the Symantec Endpoint Protection Manager System log.

To view the Web and Cloud Access Protection log on the client

1. On the client computer **Status** page, next to **Web and Cloud Access Protection**, click **Options > View Logs**.

More information:

- [What is Web and Cloud Access Protection?](#)
- [Integrating SEP and Cloud SWG \(formerly known as WSS\) using SEP Web and Cloud Access Protection](#)

What is Web and Cloud Access Protection?

Web and Cloud Access Protection protects client computers from unsafe URLs by redirecting network traffic to the Symantec Cloud Secure Web Gateway (Cloud SWG), where the Cloud SWG policies allow or block the traffic on the Symantec Endpoint Protection (SEP) client. Integration with the Cloud SWG ensures that employees cannot access malicious websites or cannot adhere to your already defined web-use policies.

How Web and Cloud Access Protection works

The Cloud SWG administrator generates an integration token in the Cloud SWG portal. You add the integration token to the Symantec Endpoint Protection Manager Web and Cloud Access Protection policy, which then pushes the integration out to the SEP clients. When client users log on to their computers, the SEP client initiates a secure connection (with a session key and a pre-shared key (PSK)) to the Cloud SWG. The SEP client then provides an *assertion* to the Cloud SWG. The assertion contains the user identity and other information about the computer, such as the OS version. This *seamless identification* means that users do not have to log on again when they access the Internet through the Captive Portal. This process allows for a per-user policy to be applied to traffic and provides risky client context to the Cloud SWG for logging and reporting.

The Symantec Endpoint Protection client handles all supported traffic in one of the following ways in one of the following ways:

- Redirects it to the Cloud SWG server.
- Blocks it.
- Allows it to continue to its destination.

Redirection methods

The Web and Cloud Access Protection policy provides the following redirection methods between the client and the Cloud SWG. The following table describes the benefits of each method, and how they work.

Table 128: Redirection methods

Method	When to use it	How it works
Tunnel (Default) (14.3 RU1 and later)	The tunnel method embeds and deploys the Cloud SWG technology into Symantec Endpoint Protection, which captures non-proxy applications. This method: • Redirects to the http and https protocols on ports 80, 443, 8080, and 8443, based on how the Cloud SWG administrator configures the behavior of the Web and Cloud Access Protection tunnel mode. • See: Set WSS Agent Network and Security Options • Redirects any application, not just web browsers. You can also choose to redirect just web traffic. • Is more robust for roaming users who change networks frequently. • Provides better security between the client computer and the data center by encrypting traffic. • Is the primary connection method to Cloud SWG. • Runs on 64-bit Intel devices. • Runs on Windows 10 64-bit version 1803 and later (14.3 RU4 and later) and Windows 10 19H2 and later (14.3 RU5 and later). • The Windows 10 Long-Term Servicing Channel (LTSC) is not supported. Microsoft intends for LTSC to be used only for specialized systems.	This method captures traffic from non-proxy aware application and enables a more granular level of security management than the PAC file redirection alone. The Cloud SWG integration token forwards more header data to identify the user that initiated the traffic, allowing for per-user traffic rules. The traffic that is redirected through the tunnel method depends on how your Cloud SWG policies are set up. For example, the policy rules can specify web traffic only, or all ports and protocols. The tunnel method also depends on your Cloud SWG license. The tunnel method installs the certificate by default because it is an encrypted tunnel. For more information on the different ways that the SEP client identifies traffic, see "Tunnel method options" at: Web and Cloud Access Protection Settings
PAC File (14.0.1 MP1 through 14.3 RU7)	The PAC File method: • Is faster than the tunnel method. • Runs on all supported Windows operating systems. • Runs on Mac computers (14.3 RU4 through 14.3 RU7) • Redirects web traffic only. • Does not encrypt traffic.	The Cloud SWG administrator configures a PAC file in the Cloud SWG portal to get a PAC file URL. The PAC file automates the web traffic redirection to the Cloud SWG and provides secure proxy settings for your web browsers. The PAC file method allows port 80 and 443 traffic (web traffic) to be redirected for inspection. However, it is unable to re-direct traffic outside of 80/443, or from applications that do not honor the proxy. Only web traffic is redirected to the WSS Agent. Every time a user accesses a website using a web browser, the browser sends all web browser traffic through the nearest cloud-hosted Cloud SWG as defined by the PAC file. Based on the rules that the PAC file defines, all supported browser traffic is handled in one of the following ways: • Without a Cloud SWG integration token, all web browser traffic visits the PAC file URL for Cloud SWG. All users abide by the same traffic rules for Cloud SWG. • With a Cloud SWG integration token, all web browser traffic visits a locally cached PAC file for Cloud SWG. Cloud SWG can determine which user the traffic came from, and direct the web traffic accordingly.

Requirements and limitations

Table 129: Technical requirements and limitations

Requirement	Description
Supported Browsers	<i>Windows:</i> • Microsoft Internet Explorer 9 - 11 • Mozilla Firefox • Google Chrome • Microsoft Edge <i>Mac: (14.3 RU4 to 14.3 RU7)</i> • Macs support Apple Safari, Google Chrome, and Mozilla Firefox. • Firefox versions 65 and later are supported in 14.2 RU1 or later.
Limitations	• The Cloud SWG is delivered on IPv4 and not IPv6. • If the Web and Cloud Access Protection feature is installed on an endpoint, the standalone Symantec WSS Agent cannot be installed. Similarly, if the WSS Agent is installed, the Web and Cloud Access Protection feature does not install. However, you can remove Web and Cloud Access Protection from existing endpoints without having to uninstall the whole client by using one of the following methods: – In Symantec Endpoint Protection Manager (SEPM), create a Client Install Feature Set that does not include Web and Cloud Access Protection and apply it to the endpoints. See: Add or remove features to existing Endpoint Protection clients – The following command-line option uses the client installation file to remove Web and Cloud Access Protection: <code>setup.exe /s /v" REMOVE=NTR /qn"</code> The tunnel method has the following limitations: • Runs on Windows 10 64-bit version 1803 and later (Semi-Annual Servicing Channel) or Windows 11. This method does not support any other Windows operating systems or the Mac client. • The Long-Term Servicing Channel (LTSC) is not supported. Microsoft intends for LTSC to be used only for specialized systems. • Outbound traffic from the Symantec Endpoint Protection client is redirected to the WSS Agent before it gets evaluated by either the client firewall or the URL reputation rules. Instead, that traffic is evaluated against the WSS Agent firewall and the URL rules. For example, if a SEP client firewall rule blocks google.com and a WSS Agent rule allows google.com, the client allows users to access google.com. Inbound local traffic to the client is still processed by the Symantec Endpoint Protection firewall. • If a client computer connects to the WSS Agent using the tunnel method and hosts virtual machines, each guest user must install the SSL certificate provided in the Cloud SWG portal. • Traffic for the local network like your home directory or Active Directory authentication is not redirected. • It is not compatible with the Microsoft DirectAccess VPN.

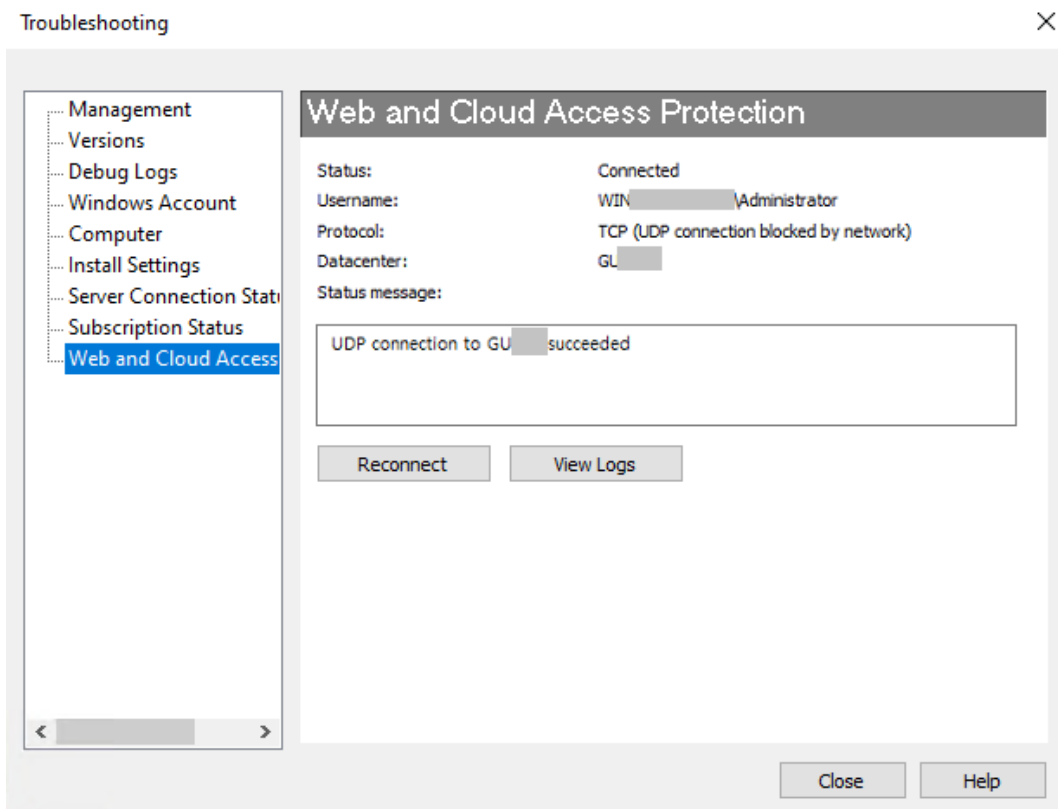
Version changes

- In 14.3 RU8, the PAC file method was removed. Because Mac clients do not use the tunnel method, Web and Cloud Access Protection only supports 14.3 RU1 to 14.3 RU7 Mac clients.
- After 14.3 RU6, the Symantec Web Security Service was renamed to Symantec Cloud Secure Web Gateway (Cloud SWG).
- In 14.3 RU5, the tunnel method includes two additional approaches for identifying traffic from the SEP client to the WSS.
- In 14.3 RU4, the tunnel method includes support for Windows 11 and HVCI-enabled Windows 64-bit devices.
- In 14.3 RU2, Network Traffic Redirection is renamed as Web and Cloud Access Protection.
- In 14.3 RU1, a new connection method is added called the tunnel method.
- In 14.3 RU1, WSS Traffic Redirection is renamed to Network Traffic Redirection.
- In 14.2, support is added to allow enhanced client authentication with WSS and a more granular control of web traffic, which is based on the user who sends it.
- In 14.2 RU2, support is added for Mac computers.
- In 14.0.1 MP1 through 14.2 RU1, WSS Traffic Redirection applies to Windows computers only.

Verifying that the Web and Cloud Access Protection tunnel method is enabled and connected on the Windows client

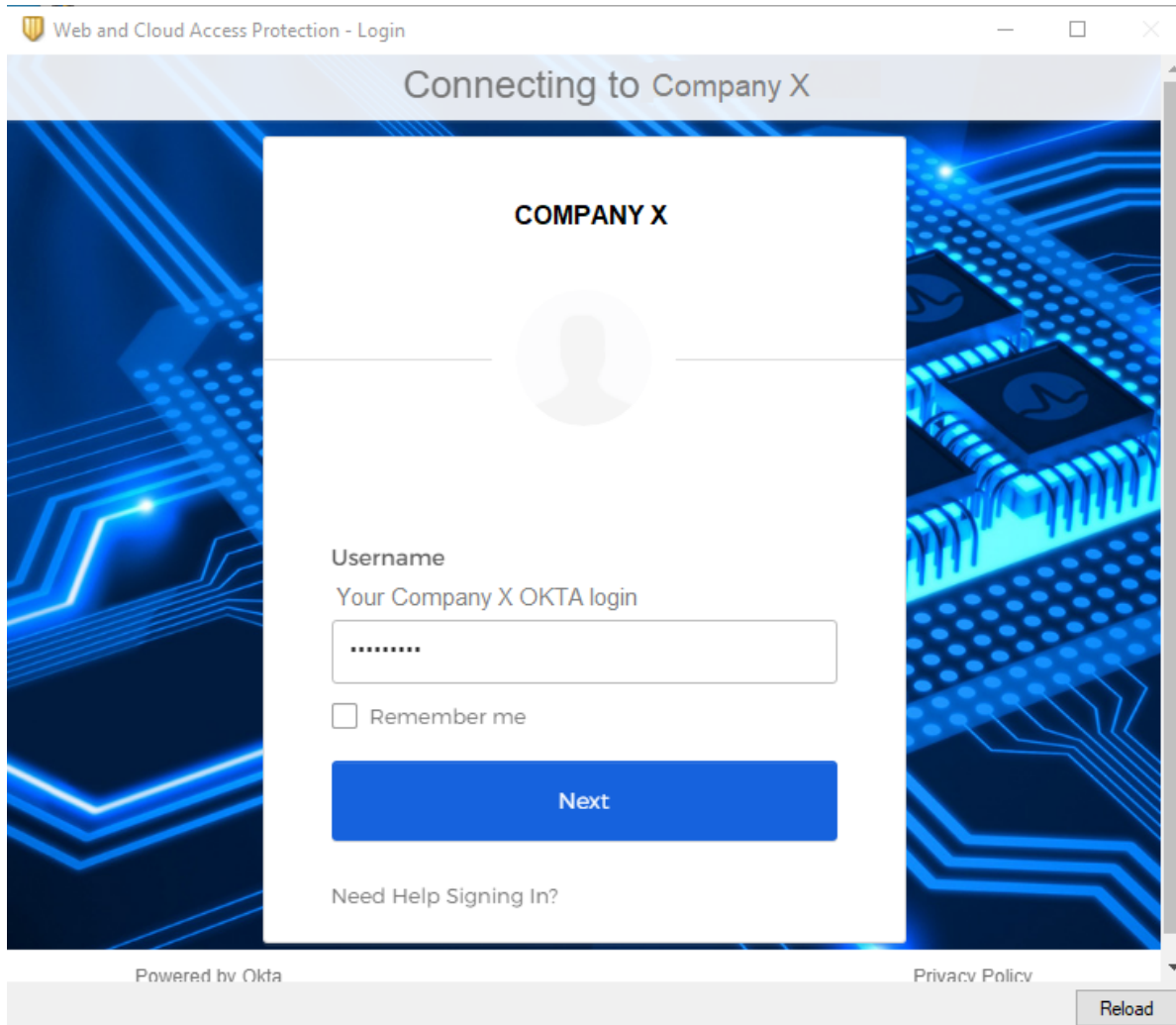
To verify that the Web and Cloud Access Protection tunnel method is enabled and connected on the Windows client

1. On the Symantec Endpoint Protection (SEP) client, click **Help > Troubleshooting > Web and Cloud Access Protection**.
If the **Status** field displays **Connected**, Web and Cloud Access Protection is enabled and connected to the Cloud SWG.



If the panel does not appear, the tunnel method is disabled on the client.

- If you enabled SAML authentication on the Cloud SWG portal, then the SEP client shows a **Web and Cloud Access Protection - Login** window with your company identity provider (IdP) page inside where the client users enter their company credentials. An identity provider (IdP) is a service that stores and manages digital identities. The following window is an example of what the client user sees. The blurred part of the window is unique to each company where the user enters their credentials. The client user should click the **Reload** button if the login window is frozen or blank.



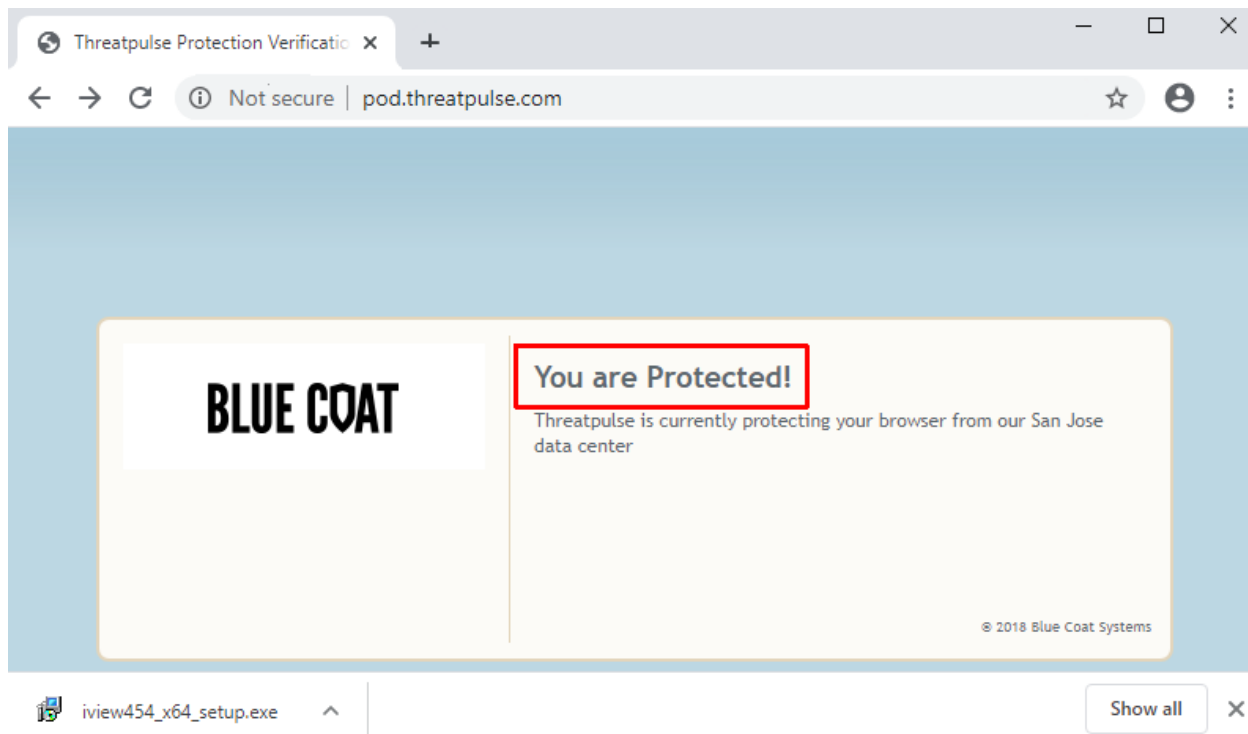
NOTE

For the SAML authentication method to run correctly, you must download and install the Microsoft Edge WebView2 Runtime2 as an administrator. Download the [Microsoft Edge Webview2 Runtime](#) application, then right-click the application and click **Run as administrator**. For Windows 11 clients, the WebView2 Runtime application is installed by default.

To use a Host Integrity policy template to install the WebView2 application, see: [Troubleshooting Web and Cloud Access Protection](#)

2. On the client, browse to the following test URL: `pod.threatpulse.com`.

If Web and Cloud Access Protection is enabled, the client user should see the following message.



Testing Web and Cloud Access Protection policies in a browser

Visiting the test websites

The Cloud SWG solution protects organizations by categorizing applications and web sites, and then allowing or denying a client user based on the Cloud SWG policy. Testing those policies is often difficult because it requires the client user to attempt to visit a site that may be dangerous, such as one categorized to have known malware. To make testing safer, Symantec has built a web site that has individual links for each category. Client users can click on a link to simulate visiting that category without risk.

To visit the test websites

1. On the client computer, open a browser window and go to <http://sitereview.symantec.com>
2. Click **Categories** and select **Test Pages**.
3. Click individual links that correspond to sites that the Cloud SWG policy allows and denies. Validate that the agent is compliant with the Cloud SWG category policy. For example, an allowed site might appear as follows:

Test Rating

This is a Symantec WebFilter test rating page categorized as

Charitable/Non-Profit

Sites that foster volunteerism for charitable causes. Also encompasses non-profit associations that cultivate philanthropic or relief efforts. Does not include organizations that attempt to influence legislation as a significant portion of their activities or organizations that campaign for, contribute to or affiliate with political organizations or candidates.

Examples: scouting.org 4-h.org ymca.net lionsclubs.org redcross.org
unicef.org pewtrusts.org cityharvest.org soles4souls.org

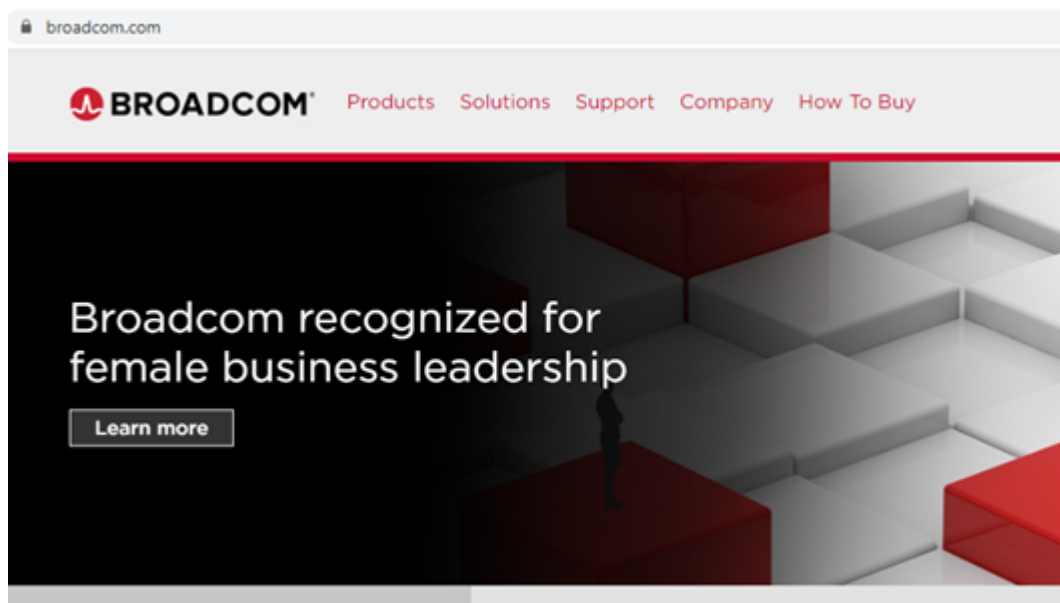
4. Click **Threat Risk** and select **Test Pages**.
The links are sorted from 1-10 with ascending simulated risk.
5. Click each link to validate that the client is compliant with the Cloud SWG risk policy.

Visiting a site allowed by policy

This example demonstrates a client user visiting a web site that the Cloud SWG policy allows. The traffic is redirected to Cloud SWG, inspected, and is passed to the web site.

To visit a site allowed by policy

1. Go to <http://www.broadcom.com>
2. Validate that the client computer opens the site.



Testing the tunnel method with Cloud SWG policies

You can test the integrated Web and Cloud Access Protection solution with the policies that the Cloud SWG administrator sets up in the Cloud SWG console. You may need to work with the Cloud SWG administrator to get a list of web sites that can be used to test each scenario, as each organization's policies are different.

Configuring the WSS Agent Block Notification Service for Web and Cloud Access Protection

The WSS Agent Block Notification Service (BNS) provides out-of-band notifications to the Symantec Endpoint Protection client when content is blocked by the Symantec CloudSOC gatelet (CASB/DLP) policies.

Technical requirements

This feature applies to deployed Symantec Endpoint Protection clients that connect through Cloud SWG accounts that are integrated with CloudSOC.

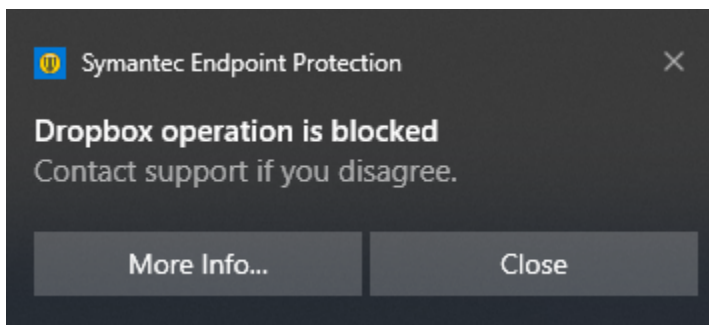
[About the Cloud SWG and CloudSOC Integration](#)

How does the Block Notification Service work?

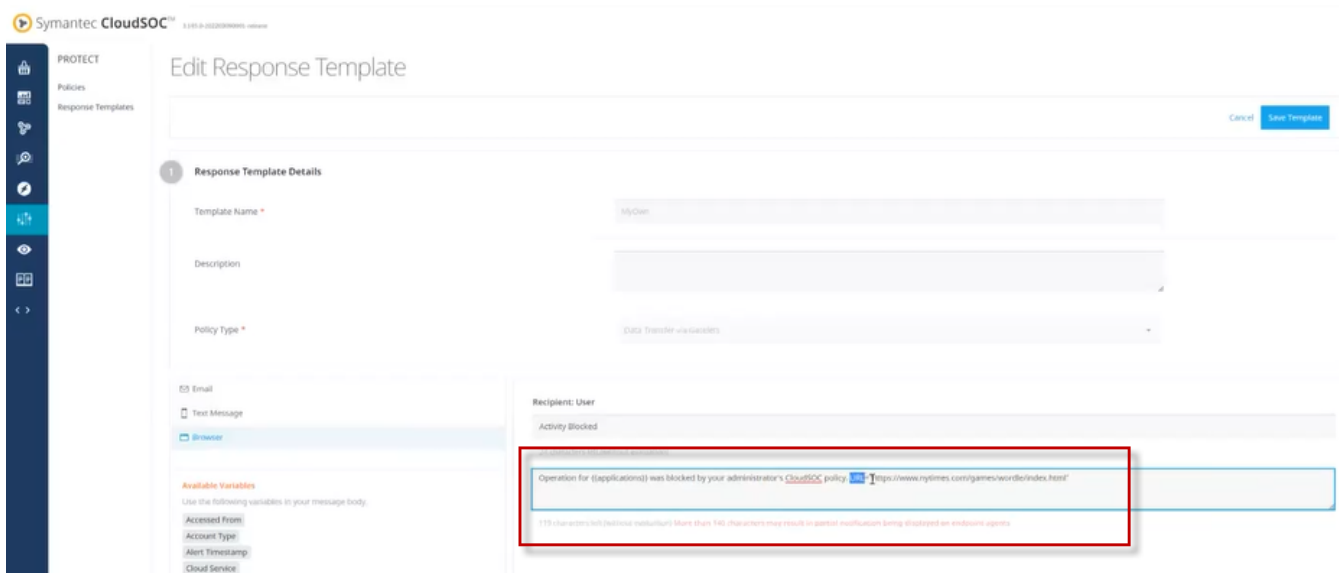
The WSS Agent BNS displays a popup message based on the policy rules that the Symantec CloudSOC administrator created. For example, the CloudSOC policy might block file downloads and enable file uploads to and from Dropbox.

The Symantec Endpoint Protection client establishes a user tunnel and connects to the WSS Agent BNS. Messages are passed through that connection to the client. The client uses the notification mechanisms that are provided by the Windows operating system (Action Center on Windows).

When the client user tries to download a file from Dropbox, they see the following type of message:



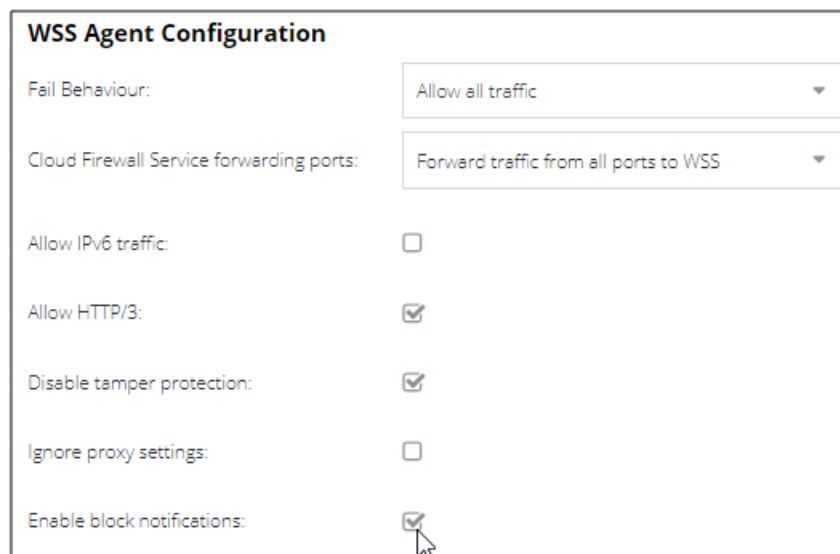
The **More Info** option appears if the CloudSOC administrator adds a URL and a message in the policy.



The BNS is not used to show a message when the client user browses to a web page that the WSS Agent blocks or allows access to.

Configuring the Block Notification Service

1. In the Cloud SWG portal, go to **Connectivity > WSS Agent**.
2. Click **Enable block notifications**.



The screenshot shows the 'WSS Agent Configuration' window with the following settings:

Setting	Value
Fail Behaviour:	Allow all traffic
Cloud Firewall Service forwarding ports:	Forward traffic from all ports to WSS
Allow IPv6 traffic:	☐
Allow HTTP/3:	☒
Disable tamper protection:	☒
Ignore proxy settings:	☐
Enable block notifications:	☒

When these elements are in place, the BNS functions. No other configuration is required.

Best practices

If the Symantec Endpoint Protection client seems to be connected and operational but is not receiving notifications, check the settings for the **Symantec WSS Agent** application delivery notifications.

Known issues

- BNS continuous pop-up occurs when there are many files to be synced with OneDrive.
Workaround—Prevent the OneDrive process from auto-starting at the Windows login: OneDrive **Settings > General** and clear the **Start OneDrive automatically when I sign in to Windows** option.

Migrating Web and Cloud Access Protection from the PAC file redirection method to the tunnel method

As of 14.3 RU8, the Web and Cloud Access Protection policy no longer provides the PAC file redirection method between the Windows or Mac client and the Symantec Cloud Secure Web Gateway (Cloud SWG). Instead, you must use the tunnel redirection method.

The following table displays the situations that you might encounter when you upgrade to 14.3 RU8 or later with the PAC file redirection method configured, and how to solve them.

Scenario	What you see	Work-around
If you upgrade from versions 14.3 RU1 through 14.3 RU7 to 14.3 RU8 or later with Web and Cloud Access Protection enabled and the PAC file method configured, Symantec Endpoint Protection Manager blocks the upgrade.	After you start the Symantec Endpoint Protection Manager Installation wizard and click Next , the following message appears: The PAC file redirection method is no longer supported. To proceed with the Symantec Endpoint Protection Manager upgrade, either convert your Web and Cloud Access Protection policies to the tunnel method or disable the policies.	1. Cancel the Installation wizard. 2. Go back to Symantec Endpoint Protection Manager and either disable the Web and Cloud Access Protection policies or configure them for the tunnel method. Whether you reconfigure the tunnel method before or after the upgrade, you must obtain a new integration token from Cloud SWG. Note: For Symantec Endpoint Protection Manager versions earlier than 14.3 RU1, you can only disable Web and Cloud Access Protection. To disable Web and Cloud Access Protection, open the policy and uncheck Enable Web and Cloud Access Protection. 3. Restart the Installation wizard. NOTES: • Symantec recommends that you disable the policies and create new policies after the upgrade. • SEP client versions earlier than 14.3 RU1 do not support the tunnel method. Therefore, after you upgrade Symantec Endpoint Protection Manager to 14.3 RU8 or later, the Web and Cloud Access Protection policy does not work on 14.3 and earlier clients. You must upgrade your clients to later versions before or after you upgrade the Symantec Endpoint Protection Manager.
If you upgrade from version 14.3 RU1 through 14.3 RU7 to 14.3 RU8 or later with the Web and Cloud Access Protection disabled and PAC file method configured, Symantec Endpoint Protection Manager allows the upgrade and converts the policies to the tunnel method.	The Management Server Upgrade wizard upgrades the Symantec Endpoint Protection Manager successfully. The Upgrade Succeeded pane notifies you that your policies were migrated, as follows: The Symantec Endpoint Protection Manager detected that one or more of the Web and Cloud Access Protection policies used the PAC file redirection method, which is no longer supported. Symantec Endpoint Protection Manager automatically converted the policies' redirection method to the tunnel method.	1. Obtain a new integration token from the Cloud SWG. 2. Paste it into the migrated Web and Cloud Access Protection policies. The PAC file redirection method token does not migrate.

Scenario	What you see	Work-around
You made a database backup from 14.3 RU1 through 14.3 RU7 with both Web and Cloud Access Protection enabled and the PAC file method configured. You then restored the database backup in Symantec Endpoint Protection Manager 14.3 RU8 or later.	After you start the restoration process, you see the following message: The Symantec Endpoint Protection Manager detected that one or more of the Web and Cloud Access Protection policies used the PAC file redirection method, which is no longer supported. The Symantec Endpoint Protection Manager automatically converted the policies redirection method to the tunnel method.	After the database restore, you must reconfigure the Web and Cloud Access Protection for the tunnel method. 1. Obtain a new integration token from the Cloud SWG. 2. Paste it into the migrated Web and Cloud Access Protection policies.
You exported a Web and Cloud Access Protection .dat file from a Symantec Endpoint Protection Manager 14.3 MP1 through 14.3 RU7, and are importing it into a Symantec Endpoint Protection Manager 14.3 RU8 or later.	Symantec Endpoint Protection Manager does not allow you to import a legacy policy with the PAC file method configured. Symantec Endpoint Protection Manager does not allow the import even if Web and Cloud Access Protection is disabled. You see the following message: The policy that you are trying to import contains the PAC file redirection method, which is no longer supported. Instead of importing a policy, create a new one.	1. Create a new policy that uses the tunnel method and a new integration token.
If you upgrade SEP clients to 14.3 RU8 or later, the functionality stays the same for client users.	The client user does not see the PAC file redirection method.	The client user can still only enable or disable Web and Cloud Access Protection if the Symantec Endpoint Protection administrator makes it available. This is no change from earlier releases.

Notes:

- In 14.3 RU7 and earlier, Symantec Endpoint Protection Manager only supported the PAC file redirection method for Mac clients. Mac support for the tunnel method will be added in a future release. To continue supporting Web and Cloud Access Protection on Mac clients, do not upgrade to Symantec Endpoint Protection Manager 14.3 RU8.
- The SES cloud server supported the PAC file redirection method until October 1, 2023.

More information

[SEP/SES "PAC File Mode" Traffic Redirector End-of-Life](#)

[Some transactions generated from SEP agents in PAC File mode are not logged](#)

Troubleshooting Web and Cloud Access Protection

You can troubleshoot common problems with Symantec Endpoint Protection (SEP) Web and Cloud Access Protection.

- [Reconnecting to the Cloud SWG](#)
- [Importing Host Integrity templates to uninstall the WSS Agent and to run the Microsoft WebView2 Runtime application](#)

To collect debug data using SymDiag for issues with Symantec Endpoint Protection clients that route traffic to the Cloud SWG, see:

Collect Cloud SWG debug data for SEP clients with SymDiag

The following table displays the issues that occur on the SEP client when Web and Cloud Access Protection is enabled.

Table 130: Web and Cloud Access Protection issues

Issue	Redirection method	Resolution
If you disable the Symantec Endpoint Protection notification area icon (system tray icon), the WSS Tunnel mode does not work for SAML authentication. When the WSS tunnel is enabled, the outgoing traffic goes through the tunnel before Symantec Endpoint Protection firewall gets a chance to inspect the traffic. Incoming traffic still gets inspected.	Tunnel	Keep the notification area icon enabled. See: On the management server: Client User Interface Mixed Control Settings: Client/Server Control Settings On the client: Displaying or hiding the notification area icon on the Symantec Endpoint Protection client On the cloud console: Hiding the Symantec Endpoint Protection client notification area icon (as of 14.3 RU9)
If you use the PAC file redirection method and upgrade to SEPM 14.3 RU8 or later, the upgrade is blocked.	PAC file	The PAC file method was removed in SEPM 14.3 RU8. See: Migrating Web and Cloud Access Protection from the PAC file redirection method to the tunnel method
When SAML authentication is enabled, some client users see one of the following errors: - The client Status page shows the following error: Web and Cloud Access Protection requires WebView2 Runtime installed. Install WebView2 Runtime or contact your administrator. - The SAML logon window shows 404 status error or timeout error.	Tunnel	This issue occurs when the client runs Windows 10 and the Microsoft Edge WebView2 Runtime application is not installed. To resolve the issue: - Make sure that the client computer runs 14.3 RU5 or later. - Download and install the Microsoft Edge WebView2 runtime application either manually or by using a Host Integrity template as an administrator. See: Importing Host Integrity templates to uninstall the WSS Agent and to run the Microsoft WebView2 Runtime application The client detects the WebView2 application installation after about 10 minutes. The client user can also click Web and Cloud Access Protection Settings > Enable Web and Cloud Access Protection if the option is available. The WebView2 Runtime application is installed with Windows 11 by default. See: WSS Agent users cannot login when SAML authentication enabled
The SAML logon window (Web and Cloud Access Protection - Login) freezes.	Tunnel	Sometimes the msedgewebview2 process may hang, which causes the SAML logon screen to freeze. To resolve this issue, perform the following steps in order: - On the Web and Cloud Access Protection - Login window, click Reload. - On the client Status page, next to Web and Cloud Access Protection, click Options > Reconnect. - Log off from the client and then log on. - Restart the client computer.
When SAML authentication is enabled but the SAML logon window appears either blank or continually reappears and does not go away.	Tunnel	On the client, click the Reconnect option.
When SAML authentication is enabled and the Symantec Endpoint Protection client cannot access the Internet, the SAML logon window (Web and Cloud Access Protection - Login) does not appear.	Tunnel	On the client, perform the following steps in order: - Click the Reconnect option to connect to the Cloud SWG and to reinitialize SAML authentication. - Restart the client.

Issue	Redirection method	Resolution
When SAML authentication is enabled, the Web and Cloud Access Protection - Login window is frozen or blank. The client users cannot enter their credentials.	Tunnel	On the client computer, perform the following steps: 1. On the Web and Cloud Access Protection - Login window, click Reload . 2. On the SEP client, click the Reconnect option.
With SAML authentication, the client user sees broken links when trying to access an HTTPS web site.	PAC file	To resolve this issue, first manually visit an HTTP site such as http://www.bbc.co.uk ; then go back to the original HTTPS site https://www.bbc.co.uk .
The web page redirects to Cloud SWG but shows an error that credential are missing.	PAC file	This problem can occur if you have provided an invalid Cloud SWG token in the Web and Cloud Access Protection policy. To resolve this issue, check that you have provided right token for the Cloud SWG integration.
PAC file could not be downloaded.	PAC file	This problem can occur if you have provided a wrong PAC file URL or your browser is preventing the file download. To resolve this issue, check the PAC file URL that you are using in the Web and Cloud Access Protection policy and verify whether the issue applies to all browsers.
The Symantec Endpoint Protection client displays one of the following errors: - The Web and Cloud Access Protection SAML login page repeatedly pops up even after the client user successfully logged in. - The Status page displays: Web and Cloud Access Protection is not functioning correctly. - The client About > Troubleshooting > Web and Cloud Access Protection page shows the following error in the Status field: 80010908	Tunnel	This issue is caused because Windows hosts that generate TLS 1.0 requests into Cloud SWG that are not responded to. WSS Agent users getting SAML window repeatedly popping up even after they have logged in

Reconnecting to the Cloud SWG

Web and Cloud Access Protection should stay continually connected to the Cloud SWG. However, there are situations where the connection gets interrupted. The Wi-Fi may go down, an internet connection gets disabled, or a data center fails. Regardless of what caused the outage, when service returns, the client user must reconnect to Cloud SWG.

Table 131: Methods for reconnecting to the Cloud SWG

Method	Description
If the Symantec Endpoint Protection client detects that the connection is broken.	- On the client, click the Status page. - At the top of the page, the stripe is green if Web and Cloud Access Protection is enabled, connected, and functioning correctly. The stripe is yellow or red if the protection is disabled or disconnected. - To reconnect to Cloud SWG, the client user should click the Fix button. 
If the client does not detect that the connection has been broken.	- On the client, click the Status page. - Next to Web and Cloud Access Protection, click Options > Reconnect. The Status field should show Connected. If not, click Reconnect.

Importing Host Integrity templates to uninstall the WSS Agent and to run the Microsoft WebView2 Runtime application

To save time, you can import Host Integrity scripts that perform the following tasks on the client computer, based on the schedule that you set:

- Uninstalls the Symantec WSS Agent from the client computers and installs the Web and Cloud Access Protection feature instead.
- Installs the Microsoft Edge WebView2 Runtime application on client computers.

Table 132: Host Integrity templates

Template	Description
Migrate Standalone WSS Agent (without uninstall token) to Symantec Endpoint Protection Client Migrate Standalone WSS Agent (with uninstall token) to Symantec Endpoint Protection Client	- If an uninstall token has been set on the Cloud SWG portal, modify the with uninstall token script to use the token that your company uses. - Make sure that these scripts do not run at the same time on the same group. Create a separate policy for each script. - Run the Host Integrity check once a day rather than every 2 minutes. Once a day is enough. Modify the Check Host Integrity every x minutes option on the Advanced Settings page. See: Advanced Settings
Install Microsoft Edge WebView2 Runtime for SAML authentication	- The Microsoft Edge WebView2 Runtime application is required on 14.3 RU5 and later clients that use SAML authentication. You can assign the Host Integrity policy to 14.3 RU4 and earlier clients without consequences. - You must install the Microsoft Edge WebView2 Runtime application on client computers that run Windows 10 but not on Windows 11.

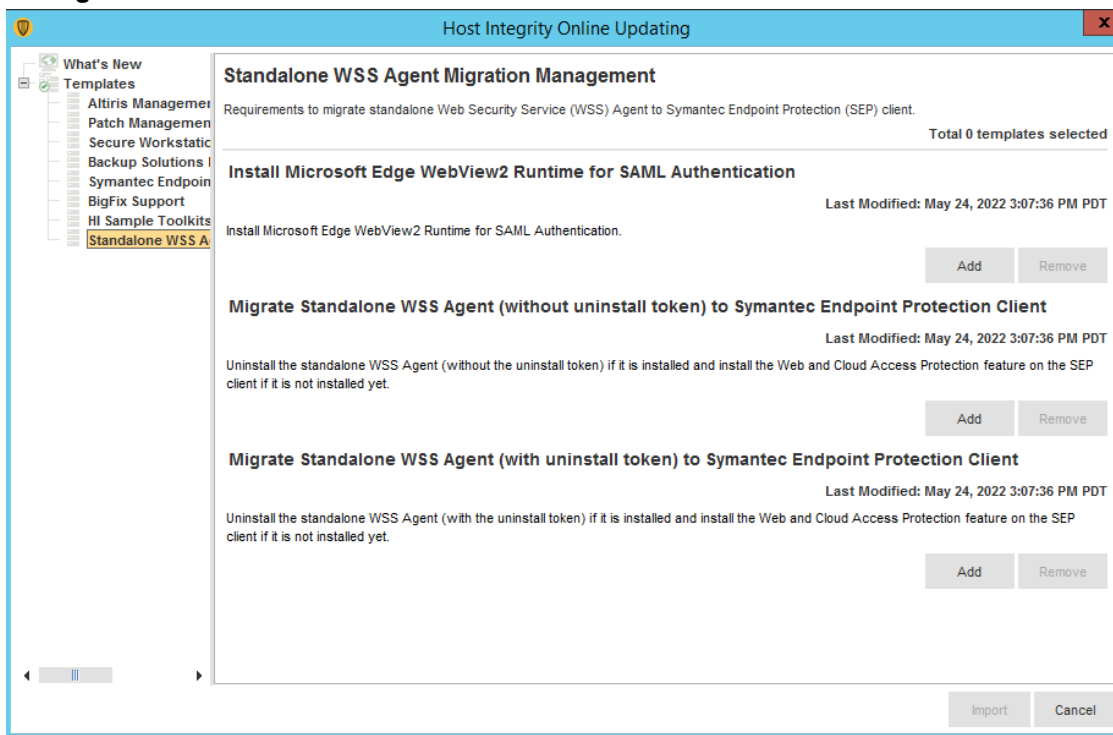
Notes:

- Read each script first to understand what it does. Make sure that you test them first with additional checks that are appropriate for your organization and environment.
- Monitor the client computers in case the script fails, and then troubleshoot.
- In the cloud console, make sure that the **Allow the Host Integrity check to pass even if this requirement fails** option is checked. You do not want the device to be quarantined or impacted by a failed migration or other requirement. You can check the reports to find the devices that failed the Host Integrity check but are marked as passed, and then troubleshoot them.

[Allowing the Host Integrity check to pass if a requirement fails](#)

To import the Host Integrity templates for Cloud SWG in the Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager console, open a Host Integrity policy and click **Requirements > Add**.
2. In the **Add Requirement** dialog box, click **Use existing templates**, and then click **OK**.
3. In the **Host Integrity Online Updating** dialog box, under **Templates**, select **Standalone WSS Agent Migration Management**.



4. Next to each template you want to add, click **Add > Import**, and then **OK**.

[Creating Host Integrity policy requirements by importing templates](#)

Managing Web and Cloud Access Protection for the Mac client

About Web and Cloud Access Protection

Web and Cloud Access Protection protects computers from unsafe web content by redirecting network traffic to the Symantec Cloud Secure Web Gateway (Cloud SWG). Your organization creates policies to allow or block the web traffic. Integration with the Cloud SWG ensures that you comply with category and content policies set by your company and blocks access to malicious websites.

How Web and Cloud Access Protection works

The Web and Cloud Access Protection policy provides the following redirection methods between the client and Cloud SWG:

- Tunnel (this method is available if you manage it from the Symantec Endpoint Security cloud console, but not from the Symantec Endpoint Protection Manager.)
All traffic is sent to the Cloud SWG for inspection.
- PAC File (removed in 14.3 RU8)
Only web traffic on ports 80 and 443 is redirected to the Cloud SWG when PAC file rules apply.

NOTE

Your administrator sets the method of traffic redirection.

NOTE

You may be prompted to input your network credentials.

Visiting websites

Web content is either displayed or blocked, according to policies of your organization. Blocked web pages are indicated with a notification page in your browser saying 'Access Denied'.

Turning on and turning off Web and Cloud Access Protection

Your administrator may ask you to disable Web and Cloud Access Protection for troubleshooting purposes.

NOTE

Your administrator may set a policy to prevent you from disabling this feature.

To turn on and turn off Web and Cloud Access Protection

1. In the Mac client, click **Advanced > Web and Cloud Access Protection**.
2. Click **Web and Cloud Access Protection**.
3. Toggle the **Web and Cloud Access Protection** option.

Verifying Web and Cloud Access Protection traffic redirection

To help with troubleshooting, you can test that the Mac client is redirecting traffic to the Cloud SWG.

To verify Web and Cloud Access Protection traffic redirection

1. Open a browser
2. Go to <https://pod.threatpulse.com>

If your traffic is being redirected, your browser displays the message, "You are protected!"

Web and Cloud Access Protection Settings

Web and Cloud Access Protection protects Windows and Mac client computers against network traffic by redirecting it to the Symantec Cloud Secure Web Gateway (Cloud SWG), where the Cloud SWG allows or blocks the traffic. The Cloud SWG allows or blocks the traffic that is based on the policy that the administrator configures in the Cloud SWG.

NOTE

To use this feature within Symantec Endpoint Protection Manager, you must have a valid Cloud SWG subscription. Contact your account representative for a subscription.

Table 133: Web and Cloud Access Protection settings

Option	Description
Enable Web and Cloud Access Protection	Enables or disables the Web and Cloud Access Protection feature on Symantec Endpoint Protection clients. You must check this option to enable it on the client. If you disable this option for the PAC File method, you can still enable the Install the Symantec Web Security Service root certificate on clients to facilitate the protection of encrypted traffic option.
Redirection Method (14.0.1 MP1 to 14.3 RU7)	- The tunnel method automatically redirects all internet traffic (ports 80, 443, 8080, and 8443) to the Cloud SWG, based on how you configure the WSS Agent behavior. Set Agent Network and Security Options You should perform thorough testing with your applications against your Cloud SWG policies. - The PAC File method redirects web only traffic (ports 80 and 443). The PAC file method was removed in 14.3 RU8. For information on the differences between the redirection methods, see: What is Web and Cloud Access Protection?

The following table displays the different methods that the Cloud SWG uses to identify the traffic from the SEP client. You configure these settings in the Cloud SWG, and then choose that method in the SEP client.

Table 134: Tunnel method options

Option	Description	Benefits	Disadvantages
Identify Traffic	Based on the console user: - Single tunnel. - Default for 14.3 RU5 and later clients. - Supported in 14.3 RU5 and later.	- Ensures that all traffic is identified as the SAML user that is logged on to the device. - Works in all cases even if SAML authentication is not used. - If the console user changes based on logging on, logging off, or fast user switching, the traffic identification method also switches.	- Does not work with endpoints that are accessed through a Remote Desktop Protocol (RDP) connection. - Does not establish a VPN tunnel until after the client user logs on. If you use a Microsoft Azure Active Directory tenant and configure it to limit access to traffic that originates from the SEP client only, the Azure AD forgotten passwords does not work.
	Using WSS SAML authentication: - Single tunnel. - Supported in 14.3 RU5 and later.	- Ensures that all traffic is identified as the assigned user regardless of the local user who is logged in to the device. - Works with endpoints that are accessed through an RDP connection. - Establishes a VPN tunnel before the client user logs on.	Requires that SAML authentication for Cloud SWG is set up before use.

Option	Description	Benefits	Disadvantages
	Based on the running process: - Multi-tunnel. - Default for 14.3 RU4. - Supported in 14.3 RU1 and later.	- Ensures that traffic is identified as the user that originally sent it on the device. - Works with endpoints that are accessed through an RDP connection. - Establishes VPN tunnels before user logs in.	- Some security applications that intercept and reinject traffic are identified as the user of the process that is reinjecting the traffic rather than the original user. - Connections can take longer because they are established on-demand when the client processes traffic from a new user. - A reconnection or disruption of a non-interactive user causes all currently established tunnels to be reconnected. - Future Web and Cloud Access Protection enhancements that require a single tunnel are not available.
Network integration token	The Cloud SWG administrator generates a randomized integration token from the Cloud SWG portal.		

Table 135: PAC File method options (14.0.1 MP1 to 14.3 RU7)

Option	Description
Proxy Auto Configuration (PAC) File URL	Indicates the URL to the Proxy Auto Configuration file, as defined by the Cloud SWG administrator. You can configure or edit this URL in Symantec Endpoint Protection Manager only.
Traffic interception port	Indicates the port in use by the local proxy service. For versions earlier than 14.2 RU1, this option only applies to Windows computers.
Network integration token	Symantec Endpoint Protection clients use the token to securely forward user ID and client-context information to the Cloud SWG. The local proxy service requires the token to parse the header information for per-user rules to allow or block the web traffic. This option allows for local caching of the PAC file. For versions earlier than 14.2 RU1, this option only applies to Windows computers.
Allow direct traffic when network protection is not available	Use this option to give users access to the web if user authentication with the Cloud SWG cloud proxy (proxySG) fails. This situation occurs if the administrator sets up a PAC file, but not the Cloud SWG roaming users. - If this option is checked and the client user fails to authenticate, the client fails open. - If this option is unchecked and the client user fails to authenticate, the client fails closed. Until users are authenticated, Web and Cloud Access Protection does not protect them. Cloud SWG attempts to authenticate the user every 5 minutes in the background. Cloud SWG then requests that the user to authenticate manually in the Cloud SWG Roaming Captive Portal. This setting is ignored until a valid authentication attempt is made. This option applies to clients 14.2 RU2 MP1 and later.

Option	Description
Enable LPS Custom PAC file	Replaces the default PAC file that is hosted by the LPS server on the client with a custom PAC file. The custom PAC file solves compatibility issues with third-party applications that do not work with a local proxy server listening on the loopback adapter. You should make all other configurations for bypass and filtering through the Cloud SWG portal. This option applies to clients 14.3 and later. Warning! If you incorrectly configure the custom PAC file option, it can prevent client users and applications from accessing the Internet. Note: The effects of the custom PAC file may not take effect immediately. You may need to restart the client.
Install the Symantec Web Security Service root certificate on clients to facilitate the protection of encrypted traffic	Installs the appropriate root certificate on Symantec Endpoint Protection clients to protect the encrypted traffic. This option can be enabled when the Enable Web and Cloud Access Protection option is disabled, which allows you to install root certificates even if the PAC file option is not selected.

Testing Symantec Endpoint Protection Manager policies

You may need to evaluate Symantec Endpoint Protection or you may need to test the policies before you download them to the client computers. You can test the following functionality using the Symantec Endpoint Protection Manager policies to make sure the product works correctly on the client computers.

Table 136: Features that you can test

Feature	See this topic
Virus and Spyware Protection	To test a default Virus and Spyware Protection policy, download the EICAR test virus from: ANTI MALWARE TESTFILE Then see: Testing a Virus and Spyware Protection policy
Behavioral analysis	Download the Socar.exe test file to verify that SONAR works correctly
Insight	How to test connectivity with Insight and Symantec Licensing servers
Intrusion Prevention	Testing a default IPS policy
Application Control	• Blocking a process from starting on client computers • Preventing users from writing to the registry on client computers • Preventing users from writing to a particular file • Adding and testing a rule that blocks a DLL • Adding and testing a rule that terminates a process

Testing a Virus and Spyware Protection policy

To test to see that the Virus and Spyware policy works, you can use the test virus file eicar.com. The EICAR test virus is a text file that the European Institute for Computer Antivirus Research (EICAR) developed. It provides an easy way and safe way to test most antivirus software. You can use it to verify that the antivirus portion of the client works.

To test a Virus and Spyware Protection policy

1. On the client computer, download the antivirus test file from the EICAR website at the following location:

[Download Anti Malware Testfile](#)

-
2. Run the EICAR test file.

A notification appears that tells you that a risk is found.

3. In Symantec Endpoint Protection Manager, on the **Monitors** page, click **Logs**.
4. On the **Logs** tab, in the **Log type** drop-down list, click **Risk**, and then click **View Log**.
5. On the **Risk Logs** page, the **Virus found event** appears.

Blocking a process from starting on client computers

The FTP client is a common way to transfer files from a server to a client computer. To prevent users from transferring files, you can add a rule that blocks a user from launching an FTP client from the command prompt.

To add a rule that blocks a process from starting on the client computer

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, in the **Rules** list, select a rule, and on the **Properties** tab, in the **Rule name** text box, type `ftp_blocked_from_cmd`.
3. To the right of **Apply this rule to the following processes**, click **Add**.
4. In the **Add Process Definition** dialog box, under **Processes name to match**, type `cmd.exe`, and then click **OK**.
5. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add Condition > Launch Process Attempts**.
6. On the **Properties** tab, in the **Description** text box, type `no ftp from cmd`.
7. To the right of **Apply this rule to the following processes**, click **Add**.
8. In the **Add Process Definition** dialog box, under **Processes name to match**, type `ftp.exe`, and then click **OK**.
9. In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Block access**, **Enable logging**, and **Notify user**.
10. Under **Notify user**, type `ftp is blocked if launched from the cmd`.
11. Click **OK** twice, and assign the policy to a group.
Test the rule.

To test a rule that blocks a process from starting on the client computer

1. On the client computer, open a command prompt.
2. In the command prompt window, type `ftp`, and then press **Enter**.
As the rule has specified, the FTP client does not open.

Preventing users from writing to the registry on client computers

You can protect a specific registry key by preventing the user from accessing or from modifying any registry keys or values in the registry. You can allow users to view the registry key, but not rename or modify the registry key.

To test the functionality, do the following:

- Add a test registry key.
- Add a rule to read but not write to the registry key.
- Try to add a new value to the registry key.

To add a test registry key

1. On the client computer, open the Registry Editor by opening a command line, then by typing `regedit`.
2. In the Registry Editor, expand `HKEY_LOCAL_MACHINE\Software`, and then create a new registry key called `test`.

To prevent users from writing to the registry on client computers

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set**, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type `HKLM_write_not_allowed_from_regedit`.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Process name to match**, type `regedit.exe`, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Registry Access Attempts**.
7. On the **Properties** tab, in the **Description** text box, type `registry access`.
8. To the right of **Apply this rule to the following processes**, click **Add**.
9. In the **Add Registry Key Definition** dialog box, in the **Registry key** text box, type `HKEY_LOCAL_MACHINE\software\test`, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, in the **Read Attempt** group box, click **Allow access**, **Enable logging**, and **Notify user**.
11. Under **Notify user**, type `reading is allowed`.
12. In the **Create, Delete, or Write Attempt** group box, click **Block access**, **Enable logging**, and **Notify user**.
13. Under **Notify user**, type `writing is blocked`.
14. Click **OK** twice, and assign the policy to a group.
Test the rule.

To test a rule that blocks you from writing to the registry

1. After you have applied the policy, on the client computer, in the Registry Editor, expand `HKEY_LOCAL_MACHINE\Software`.
2. Click the registry key that you created earlier, called `test`.
3. Right-click the test key, click **New**, and then click **String Value**.
You should not be able to add a new value to the test registry key.

Preventing users from writing to a particular file

You may want users to view but not modify a file. For example, a file may include the financial data that employees should view but not edit.

You can create an Application and Device Control rule to give users read-only access to a file. For example, you can add a rule that lets you open a text file in Notepad but does not let you edit it.

To add a rule that prevents users from writing to a particular file

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type `1.txt in c read allowed write terminate`.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Processes name to match**, type `notepad.exe`, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > File and Folder Access Attempts**.
7. On the **Properties** tab, in the **Description** text box, type `file access launched`.
8. To the right of **Apply this rule to the following processes**, click **Add**.
9. In the **Add File or Folder Definition** dialog box, in the text box in the **File or Folder Name To Match** group box, type `c:\1.txt`, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, in the **Read Attempt** group box, select **Allow access**, and then check **Enable logging** and **Notify user**.

-
11. Under **Notify user**, type `reading is allowed`.
 12. In the **Create, Delete, or Write Attempt** group box, click **Block access**, **Enable logging**, and **Notify user**.
 13. Under **Notify user**, type `writing to block Notepad`.
 14. Click **OK** twice and assign the policy to the client computer group.
Test the rule.

To test a rule that prevents users from writing to a particular file

1. On the client computer, open File Explorer, locate the `c:\` drive, and then click **File > New > Text Document**.
If you create the file by using Notepad, the file is a read-only file.
2. Rename the file as `1.txt`.
Make sure that the file is saved to the `c:\` folder.
3. In Notepad, open the `c:\1.txt` file.
You can open the file but you cannot edit it.

Adding and testing a rule that blocks a DLL

You may want to prevent the user from opening a specific application. One way to block a user from opening an application is to block a DLL that the application uses to run. To block the DLL, you can create a rule that blocks the DLL from loading. When the user tries to open the application, they cannot.

For example, the `Msvcr7.dll` file contains the program code that is used to run various Windows applications such as Microsoft WordPad. If you add a rule that blocks `Msvcr7.dll` on the client computer, you cannot open Microsoft WordPad

NOTE

Some applications that are written to be "security conscious" may interpret the DLL injection as a malicious act. Take counter measures to block the injection or remove the DLL.

To add a rule that blocks a DLL, open an Application Control policy

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type `Block user from opening Microsoft WordPad`.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Processes name to match**, type `C:\Program Files\Windows NT\Accessories\wordpad.exe`, and then click **OK**.
6. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Condition > Load DLL Attempts**.
7. On the **Properties** tab, in the **Description** text box, type `dll blocked`.
8. To the right of **Apply to the following DLLs**, click **Add**.
9. In the **Add DLL Definition** dialog box, in the text box in the **DLL name to match** group box, type `MSVCRT.dll`, and then click **OK**.
10. In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Block access**, **Enable logging**, and **Notify user**.
11. Under **Notify user**, type `Should not be able to load WordPad`.
12. Click **OK** twice and assign the policy to the client computer group.
Test the rule.

To test a rule that blocks a DLL

1. On the client computer, try to open Microsoft WordPad.

Adding and testing a rule that terminates a process

Process Explorer is a tool that displays the DLL processes that have opened or loaded, and what resources the processes use. You can also use the Process Explorer to terminate a process. You can add a rule to terminate the Process Explorer if the user uses Process Explorer to try to terminate the Calculator application.

To add a rule that terminates a process

1. Open an Application Control policy, and on the **Application Control** pane, click **Add**.
2. In the **Application Control Rule Set** dialog box, under the **Rules** list, click **Add > Add Rule**.
3. On the **Properties** tab, in the **Rule name** text box, type `Terminates Process Explorer if Process Explorer tries to terminate calc.exe`.
4. To the right of **Apply this rule to the following processes**, click **Add**.
5. In the **Add Process Definition** dialog box, under **Processes name to match**, type `procexp.exe`, and then click **OK**.
6. On the **Properties** tab, in the **Description** text box, type `dll stopped`.
7. To the right of **Apply this rule to the following processes**, click **Add**.
8. In the **Add Process Definition** dialog box, in the text box in the **Process name to match** group box, type `calc.exe`, and then click **OK**.
9. In the **Application Control Rule Set** dialog box, on the **Actions** tab, click **Terminate process**, **Enable logging**, and **Notify user**.
10. Under **Notify user**, type `If you try to terminate the calc from procexp, procexp terminates`.
11. Click **OK** twice, and assign the policy to a group.
Test the rule.

To test a rule that terminates a process

1. On the client computer, download and run a free version of the Process Explorer from the following URL:
[Process Explorer](#)
2. In Windows, open the Calculator.
3. Open the Process Explorer.
4. In the **Process Explorer** window, right-click the `calc.exe` process, and then click **Kill Process**.
The Process Explorer is terminated.

Testing a default IPS policy

To test the default IPS policy, you must first trigger an event on the client computer.

To test a default IPS policy

1. Rename an executable file (.exe) to a jpeg (.jpg).
2. Upload the .jpg file to a web server\site.
3. On the client computer, use a web browser to open the renamed executable file.

NOTE

To open the renamed executable file, you must access the web server\site using the IP address. For example, you would type: `http://web server IP address/renamed executable.jpg`

4. On the client, if the IPS policy works correctly, the following events occur:
 - You should not be able to open the .jpg file.
 - A message in the notification area icon states that the client blocked the .jpg file.
 - You can open the Security log and look for a log entry that states that the client blocked the .jpg file.

Managing the client-server connection

Make sure that the management server delivers content to the clients.

After you install the client, the management server automatically connects to the client computer.

Table 137: Tasks to manage connections between the management server and the clients

Action	Description
Check whether the client is connected to the management server	You can check the client status icon in the client and in the management console. The status icon shows whether the client and the server communicate. See: Checking whether the client is connected to the management server and is protected A computer may have the client software installed, but does not have the correct communications file. See: • How does the client computer and the management server communicate? • How do I replace the client-server communications file on the client computer?
Check that the client gets policy updates	Check that the client computers get the most current policy updates by checking the policy serial number in the client and in the management console. The policy serial number should match if the client can communicate with the server and receives regular policy updates. You can perform a manual policy update and then check the policy serial numbers against each other. See: • Using the policy serial number to check client-server communication • Updating client policies
Change which method you use to download policies and content to the clients	You can configure the management server to push down policies to the client or for the clients to pull the policies from the management server. See: Updating policies and content on the client using push mode or pull mode
Decide whether to use the default management server list	You can work with an alternative list of management servers for failover and load balancing. The management server list provides a list of multiple management servers that clients can connect to. See: Configuring a management server list for load balancing
Configure communication settings for a location	You can configure separate communication settings for locations and for groups. See: Configuring communication settings for a location
Troubleshoot management server connectivity problems	If the management server and the client do not connect, you can troubleshoot connection problems. See: Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client

For more information, see the following article:

[About the communication ports that Symantec Endpoint Protection uses](#)

Improving client and server performance

Symantec Endpoint Protection Manager includes various features that enable you to increase the client performance and server performance while still maintaining a high level of security.

Table 138: Tasks to improve performance on the server and on the client

Task	Description
Change client-server communication settings	Use pull mode instead of push mode to control how often the management server downloads policies and content updates to the client computers. In pull mode, the management server can support more clients. Increase the heartbeat interval so that the client and the server communicate less frequently. For fewer than 100 clients per server, increase the heartbeat to 15-30 minutes. For 100 to 1,000 clients, increase the heartbeat to 30-60 minutes. Larger networks might need a longer heartbeat interval. Increase the download randomization to between one and three times the heartbeat interval. See: • Updating policies and content on the client using push mode or pull mode For more information about setting heartbeat intervals, see the following white paper: • Symantec Endpoint Sizing and Scalability Best Practices
Randomize and reduce the number of content updates	Content updates vary in size and frequency, depending on the content type and availability. You can reduce the effect of downloading and importing a full set of content updates by using the following methods: • Distribute the client load across multiple management servers. See: • Configuring a management server list for load balancing • Use alternative methods to distribute the content, such as a Group Update Provider or third-party distribution tools. A Group Update Provider helps you conserve bandwidth by offloading processing power from the server to a client that downloads the content. See: – Using Group Update Providers to distribute content to clients – Using third-party distribution tools to update client computers • Randomize the time when LiveUpdate downloads content to the client computers. See: – Randomizing content downloads from a LiveUpdate server – Randomizing content downloads from the default management server or a Group Update Provider • Download content updates when users are not actively using the client computer. See: • Configuring Windows client updates to run when client computers are idle
Adjust scans to improve computer performance	You can change some scan settings to improve the computers' performance without reducing protection. For example, you can configure scans to ignore trusted files or to run when the computer is idle. See: • Adjusting scans to improve computer performance • Customizing Auto-Protect for Windows clients • Advanced Scanning and Monitoring

Task	Description
Reduce database client log volume	You can configure the logging options to optimize storage requirements and comply with company policies that control retention of logged data. The database receives and stores a constant flow of entries into its log files. You must manage the data that is stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash. You can reduce the volume of log data by performing the following tasks: • Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. See: Specifying client log size and which logs to upload to the management server • Specify how many log entries the client computer can keep in the database, and how long to keep them. See: Specifying the log size and how long to keep log entries in the database • Filter the less important risk events and system events out so that less data is forwarded to the server. See: Modifying log handling and notification settings on Windows computers • Reduce the number of clients that each management server manages. See: — Configuring a management server list for load balancing — Installing Symantec Endpoint Protection Manager • Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See: Updating policies and content on the client using push mode or pull mode • Increase the amount of hard disk space in the directory where the log data is stored before being written to the database. See: About increasing the disk space on the server for client log data
Perform database maintenance tasks	To increase the speed of communication between the client and the server, you should schedule regular database maintenance tasks. See: Scheduling automatic database maintenance tasks

About server certificates

Certificates are the industry standard for authenticating and encrypting sensitive data. To prevent the reading of information as it passes through routers in the network, data should be encrypted.

To communicate with the clients, the management server uses a server certificate. For the management server to identify and authenticate itself with a server certificate, Symantec Endpoint Protection Manager encrypts the data by default. However, there are situations where you must disable encryption between the server and the client. See:

[Update the server certificate on the management server without breaking communications with the client](#)

You may also want to back up the certificate as a safety precaution. If the management server is damaged or you forget the keystore password, you can easily retrieve the password. See:

- [Backing up a server certificate](#)
- [Updating or restoring a server certificate](#)
- [Generating a new server certificate](#)

The management server supports the following types of certificates:

- JKS Keystore file (.jks) (default)
A Java tool that is called keytool.exe generates the keystore file. The Java Cryptography Extension (.jceks) format requires a specific version of the Java Runtime Environment (JRE). The management server supports only a .jceks keystore file that is generated with the same version as the Java Development Kit on the management server.
The keystore file must contain both a certificate and a private key. The keystore password must be the same as the key password. You can locate the password in the following file:

SEPM_Install\Server Private Key Backup\recovery_timestamp.zip

SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

- PKCS12 keystore file (.pfx and .p12)
- Certificate and private key file (.der and .pem format)

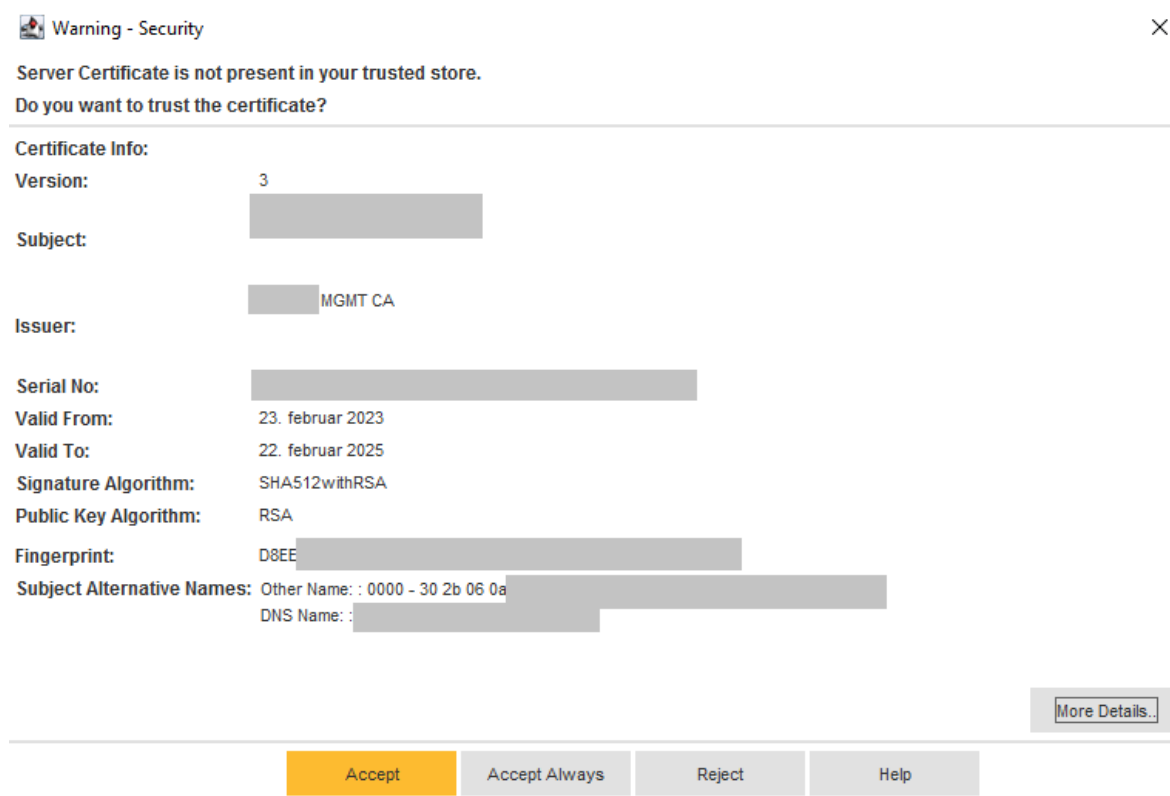
Symantec supports unencrypted certificates and private keys in the .der or the .pem format. Pkcs8-encrypted private keys are not supported.

NOTE

When the Symantec Endpoint Protection client connects to the management server and you see the following cURL error: `revocation server is offline`. This issue could be caused by a certificate/PKI issue, such as a [misconfigured AIA/CDP extension](#) that forces a check with a [CRL](#).

Accepting the self-signed server certificate for Symantec Endpoint Protection Manager

When you install Symantec Endpoint Protection Manager, a self-signed certificate for the pages that are rendered in a browser is included as part of the installation. When you first access these pages from a remote console, you must accept the self-signed certificate for the management server pages to display.



The certificates are stored separately for each user. Each administrator account must accept the certificate for each remote location from which they connect to the management server.

To accept the certificate

- Click **Accept** or **Accept Always**.

The local console trusts the certificate on the management server by default. However, on the remote management console, this message may continue to appear for each Symantec Endpoint Protection Manager logon attempt.

NOTE

If you reject the certificate, you may see an error message when you log on to Symantec Endpoint Protection Manager. This usually occurs when an administrator on a replication partner did not accept the certificate.

Certain events, such as a hostname mismatch with the certificate Common Name (CN) causes the the certificate in the Java keystore, located by default in `\tomcat\etc` to not be trusted. The prompt should allow you to add the certificate into the Java keystore, however, file access issues can prevent this from occurring. Review the `scm-ui log` located in the user temporary directory in Windows (`%temp%`) to investigate further.

For instructions to add the security certificate to the web browser, you need to install the manager's certificate as a trusted root CA. See:

[Certificate error when using a web browser to view the Endpoint Protection Manager console](#)

More information

[Logging on to the Symantec Endpoint Protection Manager console](#)

Updating the server certificate on the management server without breaking communications with the client

Symantec Endpoint Protection Manager uses a certificate to authenticate communications with the Symantec Endpoint Protection clients. The certificate also digitally signs the policy files and installation packages that the client downloads from it. The clients store a cached copy of the certificate in the management server list. If the certificate is corrupted or invalid, the client cannot communicate with the server.

If you disable secure communications, then the clients can still communicate with the server, but they do not authenticate communications from the management server. After you update the certificate and the clients check in and receive it, enable secure communications again.

If the management server does break communications with the clients, you restore orphan clients using the communication update package.

[Restoring client-server communications with Communication Update Package Deployment](#)

[Restoring client-server communication settings with the SylinkDrop tool](#)

Update the server certificate on one management server

To update the server certificate for one management server in a site

1. In the console, click **Policies > Policy Components > Management Server Lists**.
2. Under **Tasks**, click **Copy the List**, and then click **Paste List**.
3. Right-click the copy of the list, click **Assign**, select the same groups as the original list, and then click **Assign**.
4. Click **Clients > Policies > General**.
5. On the **Security Settings** tab, uncheck **Enable secure communications between the management server and clients by using digital certificates for authentication**, and then click **OK**.
6. Wait at least 24 hours or longer before you proceed to the next step.
Waiting up to one week is recommended, which allows as many clients as possible to download the new communication details from the management server. If you update your certificate prematurely, you orphan clients and you must manually reconnect them using the Communication Update Package.
Make sure that you also configure this setting for the groups that do not inherit from a parent group.
7. Update the server certificate.
[Updating or restoring a server certificate](#)
8. Click **OK**.

To reenable the original settings, wait at least 24 hours, recheck **Enable secure communications between the management server and clients by using digital certificates for authentication**, and then reassign the original management server list back to your groups.

Update the server certificate on multiple management servers

When you update the certificate on a site with multiple management servers and you use failover or load balancing, the certificate updates on the management server list. During the process of failover or load balancing, the client receives the updated management server list and the new certificate.

To update the server certificate on a multi-management server site

1. In the console, ensure that your clients are configured to load balance or failover to at least one other Symantec Endpoint Protection Manager.

[Setting up failover and load balancing](#)

If you cannot enable load balancing or failover, use the single management server site procedure to first disable then reenable secure communications.

WARNING

Due to a change in the communication module, client versions 14.2/14.2.1 only cannot use this method to update the server certificate. To avoid breaking communication with these clients, use the single management server site procedure for these client versions, even for multi-management server sites.

2. Update the server certificate on Symantec Endpoint Protection Manager.
[Updating or restoring a server certificate](#)
3. Wait at least three heartbeat cycles, and then update the server certificate on the next Symantec Endpoint Protection Manager on the site.
4. Repeat steps 2 and 3 until each Symantec Endpoint Protection Manager on the site has the new certificate.

NOTE

Users who are out of the office or on leave may not receive these updates on their device because it is offline. Many institutions run the failover method for 30 days or more to catch as many out-of-office clients as possible. You may want to leave one Symantec Endpoint Protection Manager running for 90 days with the old certificate to ensure that those users are not orphaned.

For more information, see: [About server certificates](#)

Updating or restoring a server certificate

The server certificate encrypts and decrypts files between the server and the client. The client connects to the server with an encryption key, downloads a file, and then decrypts the key to verify its authenticity. If you change the certificate on the server without manually updating the client, the encrypted connection between the server and the client breaks. This problem is called orphaning clients.

NOTE

When you try to update the Symantec Endpoint Protection Manager (SEPM) certificate using the Manage Server Certificate Wizard, you may see the following error: `invalid private file key`. The SEPM may be encountering an error processing the file, or the certificate is invalid. See: [Error "Invalid private key file \[0x840b0000\]" during update of Endpoint Protection Manager certificate](#)

When should I update the server certificate?

You must update the server certificate in the following situations:

- You reinstall Symantec Endpoint Protection Manager without using the recovery file. You update the certificate to restore a previous certificate that clients already use. See:

Installing Symantec Endpoint Protection Manager

- You replace one management server with another management server and use the same IP address and server name.
- You apply the wrong server certificate (.JKS) after disaster recovery.
- You purchased a different certificate and want to use that certificate instead of the default .JKS certificate. See: [About server certificates](#)

Before you import a server certificate

Before you import a new certificate in step 6, you must:

1. Break the replication relationship (optional). If the management server you want to update replicates with other management servers, break the replication relationship. See: [Disabling replication and restoring replication before and after an upgrade](#)
2. Disable the server certificate verification. When you disable the verification, the clients stay connected while the server updates the server certificate.

[Update the server certificate on the management server without breaking communications with the client](#)

The process of deploying the updated policy may take a week or longer, depending on the following factors:

- The number of clients that connect to the management server. Large installations may take several days to complete the process because the managed computers must be online to receive the new policy.
 - Some users may be on vacation with their computers offline.
3. Make sure that the new certificate is valid.
 4. Make sure that the server name in the new certificate matches the Subject Alternate Name(s) (SAN) listed in the existing certificate.
If the server name is an invalid host name, fully qualified domain name (FQDN), or IP address, or if it does not match one of the Subject Alternate Name(s) (SANs) listed in the server certificate, you must rename the server or update your server certificate.
[Troubleshooting: Your server certificate is not valid because the computer host name or IP address changed \(14.3 RU8 or later\)](#)

Updating a server certificate

To update or restore a server certificate

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, under **Local Site**, click the management server for which you want to update the server certificate.
3. Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
4. In the **Manage Server Certificate** panel, click **Update the server certificate**, and then **Next**.
5. When you see the following message: `Another certificate is already in use`, choose one of the following options:
 - If you need to complete the following tasks, click **No > Cancel**.
 - Temporarily disable server verification.
 - Make sure the server name in the new certificate and the existing certificate match.
[Troubleshooting: Your server certificate is not valid because the computer host name or IP address changed \(14.3 RU8 or later\)](#)
After you complete these tasks, restart the procedure.
 - If you have completed these tasks, click **Yes**.
6. In the **Update Server Certificate** panel, choose the certificate type that you want to import, and then click **Next**.
7. For each certificate type, following the instructions on each panel and then click **Finish**.

Backup server certificates are in <SEPM_Install>\Server Private Key Backup \recovery_timestamp.zip. You can locate the password for the keystore file in the settings.properties file within the same .zip file. The password appears in the keystore.password= line.

SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

8. Restart the following services to use the new certificate:
 - The Symantec Endpoint Protection Manager service
 - The Symantec Endpoint Protection Manager Webserver service
 - The Symantec Endpoint Protection Manager API service
 - [Stopping and starting the management server service](#)
 - [Stopping and starting the Apache Web server](#)
9. Reenable server certificate verification.
10. (Optional). Restore the replication relationship, if you use replication in your environment.

More information:

[Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate \(14.3 RU9 or later\)](#)

[Symantec Endpoint Protection Manager detected that the configured replication partner requires host name verification to be disabled \(14.3 RU9 or later\)](#)

Checking whether the client is connected to the management server and is protected

After you install the client, check whether the clients are online and connected to the Symantec Endpoint Protection Manager. You can check the connection status on both the console and on the client.

To check the client-management server connection on the Symantec Endpoint Protection client,

1. On the client computer, do one of the following tasks:
 - The client shield in the computer's taskbar has a green dot:

 - Open the client and look on the Status screen, which states that **Your computer is protected** and displays a green check mark:

 - Open the client and click **Help > Troubleshooting**.

For more information, see: [Symantec Endpoint Protection client status icons](#)

To check the client-management server connection in Symantec Endpoint Protection Manager

1. In the console, click **Clients** and select the target group.
2. On the **Clients** tab, clients that are connected display an icon with a green dot in the **Name** column and display a health state of **Online**:



NOTE

Clients that connect through Symantec Endpoint Protection Manager may not immediately display the correct online status in the cloud console. Allow for 5-10 minutes after the online status changes to see an accurate reflection of the current status.

Table 139: Client status icons in the management console on the Clients > Clients tab > Name column

Icon	Description
	The client software installation failed.
	- The client can communicate with Symantec Endpoint Protection Manager. The health state is Online. - The client is in computer mode.
	- The client cannot communicate with Symantec Endpoint Protection Manager. The health state is Offline. - The client is in computer mode. - The client may have been added from the console, and may not have any Symantec client software installed.
	- The client can communicate with Symantec Endpoint Protection Manager. - The client is in computer mode. - The client is an unmanaged detector.
	- The client cannot communicate with Symantec Endpoint Protection Manager. - The client is in computer mode. - The client is an unmanaged detector.
	- The client can communicate with Symantec Endpoint Protection Manager. - The client is in user mode.
	- The client cannot communicate with Symantec Endpoint Protection Manager. - The client is in user mode. - The client may have been added from the console, and may not have any Symantec client software installed.
	- The client can communicate with Symantec Endpoint Protection Manager at another site. - The client is in computer mode.
	- The client can communicate with Symantec Endpoint Protection Manager at another site. - The client is in computer mode. - The client is an unmanaged detector.
	- The client can communicate with Symantec Endpoint Protection Manager at another site. - The client is in user mode

More information

[Viewing the protection status of client computers](#)

Symantec Endpoint Protection client status icons

You can check the notification area icon on the client to determine whether the client is connected to a management server and adequately protected. The notification area icon is sometimes referred to as the system tray icon.

The icon is located in the lower-right hand corner of the client computer desktop. You can also right-click this icon to display frequently used commands.

NOTE

On managed clients, the notification area icon does not appear if the administrator has configured it to be unavailable.

[Allowing users to change settings on the Symantec Endpoint Protection client user interface](#)

Table 140: Client status icons

Icon	Description
	The client runs with no problems. It is either offline or unmanaged. Unmanaged clients are not connected to a management server.
	The client runs with no problems. It is connected to and communicates with the server. All components of the security policy protect the computer.
	The client has a minor problem. For example, the virus definitions may be out of date.
	The client does not run, has a major problem, has an expired license, or has at least one protection technology disabled.

More information

- [Displaying or hiding the notification area icon on the Symantec Endpoint Protection client](#)
- [Understanding the Symantec Endpoint Protection client Status page](#)

Using the policy serial number to check client-server communication

To check whether the server and client communicate, check the policy serial number on the console and on the client. If the client communicates with the management server and receives regular policy updates, the serial numbers should match.

If the policy serial numbers do not match, you can try to manually update the policies on the client computer and check the troubleshooting logs. See:

- [Updating client policies](#)
- [Updating policies and content on the client using push mode or pull mode](#)

To view the policy serial number in the console

1. In the console, click **Clients**.
2. Under **Clients**, select the relevant group.

NOTE

The policy serial number and the policy date also appear at the bottom of the details list on the **Details** tab.

To view the policy serial number on the client computer

1. On the client computer, in the client, click **Help > Troubleshooting**.
2. On the **Management** tab, locate the policy serial number.
The serial number should match the serial number on the console for the group that the client computer is in.

More information

[Performing the tasks that are common to all policies](#)

Updating policies and content on the client using push mode or pull mode

Learn more about the following topics:

- [Deciding whether to use pull mode or push mode to connect between Symantec Endpoint Protection Manager and the clients](#)
- [Configuring push mode or pull mode for a group or a location](#)

Deciding whether to use pull mode or push mode to connect between Symantec Endpoint Protection Manager and the clients

When you configure policies on the management server, you need to have the updated policies downloaded to the client computers. In the console, you can configure client computers to use either of the following update methods:

Pull mode	The client computer connects to the management server periodically, depending on the frequency of the heartbeat setting. The client computer checks the status of the management server when the client connects.
Push mode	The client computer establishes a constant HTTP connection to the management server. Whenever a change occurs in the management server status, it notifies the client computer immediately.

In either mode, the client computer takes the corresponding action, based on the change in the status of the management server. Because it requires a constant connection, push mode requires a large amount of network bandwidth. Client computers that are configured to use pull mode require less bandwidth.

The heartbeat protocol defines the frequency at which client computers upload data such as log entries and download policies. The first heartbeat occurs immediately after the client starts. The next heartbeat occurs at the heartbeat frequency that you set.

The heartbeat frequency is a key factor in the number of clients that each Symantec Endpoint Protection Manager can support. If you set a heartbeat frequency to 30 minutes or less, it limits the total number of clients that Symantec Endpoint Protection Manager can support. For deployments of 1,000 clients or more, Symantec recommends that you set the heartbeat frequency to the maximum length of time possible. Symantec recommends that you use the longest interval that still meets your company's security requirements. For example, if you want to update policies and gather logs on a daily basis, then you might set the heartbeat frequency to 24 hours. Assess the proper configuration, hardware, and network architecture necessary for your network environment.

NOTE

You can also update policies manually on a client computer.

For more information, see:

- [Using the policy serial number to check client-server communication](#)
- [Communication ports for Symantec Endpoint Protection](#)

Configuring push mode or pull mode for a group or a location

You can specify whether Symantec Endpoint Protection Manager pushes the policy down to the clients or that the clients pull the policy from Symantec Endpoint Protection Manager. The default setting is push mode. If you select pull mode, then by default, clients connect to the management server every 5 minutes, but you can change this default heartbeat interval. See:

[Performing the tasks that are common to all policies](#)

You can set the mode for a group or for a location.

To configure push mode or pull mode for a group

1. In the console, click **Clients**.
2. Under **Clients**, select the group for which you want to specify whether to push or pull policies.
3. Click **Policies**.
4. Uncheck **Inherit policies and setting from the parent group "group name"**.
5. Under **Location-independent Policies and Settings** pane, under **Settings**, click **Communications Settings**.
6. In the **Communications Settings for group name** dialog box, under **Download**, verify that **Download policies and content from the management server** is checked.
7. Do one of the following tasks:

-
- Click **Push mode**.
 - Click **Pull mode** and under **Heartbeat Interval**, set the number of minutes or hours.
8. Click **OK**.

To specify push mode or pull mode for a location

1. In the console, click **Clients**.
2. Under **Clients**, select the group for which you want to specify whether to push or pull policies.
3. Click **Policies**.
4. Uncheck **Inherit policies and setting from the parent group "group name"**.
5. Under **Location-specific Policies and Settings**, under **Location-specific Policies** for the location you want to modify, expand **Location-specific Settings**.
6. Under **Location-specific Settings**, to the right of **Communications Settings**, click **Tasks** and uncheck **Use Group Communications Settings**.
7. To the right of **Communications Settings**, click **Local - Push** or **(Local - Pull)**.
8. Do one of the following tasks:
 - Click **Push mode**.
 - Click **Pull mode** and under **Heartbeat Interval**, set the number of minutes or hours.
9. Click **OK**.

More information

[Performing the tasks that are common to all policies](#)

How does the client computer and the management server communicate?

Symantec Endpoint Protection Manager connects to the client with a communications file called Sylink.xml. The Sylink.xml file includes the communication settings such as the IP address of the management server and the heartbeat interval. After you install a client installation package on to the client computers, the client and the server automatically communicate.

The sylink file performs many of its functions during the heartbeat. The heartbeat is the frequency at which client computers upload logs to the management server, and download policies and commands.

The sylink file contains:

- The public certificate for all management servers.
- The KCS, or encryption key.
- The Domain ID that each client belongs to.

NOTE

Do not edit the sylink file. If you change the settings, the management server overwrites most settings the next time the client connects to the management server.

For more information, see:

[Updating policies and content on the client using push mode or pull mode](#)

Troubleshooting Sylink communication

In version 14.2, the communications module was upgraded, and includes new log files. You can use this information to troubleshoot communication issues between Symantec Endpoint Protection Manager and the clients.

The 14.2 communications module works with all client types, including Windows, Mac, and Linux, and has improved IPv6 support.

NOTE

As of version 14.2, the communication module only honors system proxy information.

To view the log files for the communications module

1. On the Windows client, in the following folder:

`C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data`

You can view the following files:

- **For client registration:**

- `RegistrationInfo.xml`

Client registration metadata that the client submits to Symantec Endpoint Protection Manager.

- `Registration.xml`

Client registration metadata that Symantec Endpoint Protection Manager returns to the client.

- `State.xml`

Includes internal settings, such as the management server IP address.

- **For the communications module logs:**

`\Logs\cve.log` and `\Logs\cve-actions.log`

Use these logs to troubleshoot communication between Symantec Endpoint Protection Manager and the client.

Send these logs to Technical Support if asked.

- **For the opstate status:**

Appears in the logs in the `\Pending` and `\Sent` folders

To configure the communication module logs

1. Open the Windows Registry Editor, click **Start > Run**, type `regedit`, and then click **OK**.

2. To enable the `cve.log` or `cve-actions.log`, open the following Windows registry key:

`[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink
REG_DWORD: CVELogLevel`

Use any of the following values:

- 1 = Debug
- 2 = Info
- 3 = Warning
- 4 = Error
- 5 = Fatal

If the registry key is not present or does not have a valid value, it defaults to 4. The installation default is also 4.

For example, you can type:

- 32-bit: `[HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink]
"CVELogLevel"=dword:00000001`

- 64-bit (14.3 RU4 or earlier): `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection`

- 64-bit (14.3 RU5 or later): `[HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK
\SyLink] "CVELogLevel"=dword:00000001`

3. To control the size of these logs, use the following registry value:

`[HKEY_LOCAL_MACHINE\SOFTWARE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK
\SyLink] REG_DWORD: CVELogSizeDB`

The default size is 250 MB.

More information

-
- [How to enable Communication Module logging in Endpoint Protection 14.2](#)
 - [How to enable Sylink debugging for Endpoint Protection clients \(14.1 and earlier\)](#)

Replacing the client-server communications file on the client computer

When should I replace the client-server communications file on the client computer?

Normally you do not need to replace the Sylink.xml file. However, you should replace the existing Sylink.xml file on the client computer in the following situations:

- The client and the management server do not communicate. For information about how to check the communication, see:
[Checking the connection to the management server on the client computer](#)
- You want to convert an unmanaged client to a managed client. If a user installs a client from the installation file, the client is unmanaged and does not communicate with the management server. See:
[About managed and unmanaged clients](#)
[How to convert an unmanaged Symantec Endpoint Protection for Macintosh client to managed](#)
You can also reinstall the client software on the computer as a managed computer.
- You must reconnect a previously orphaned client. For example, if the hard drive that the management server is installed on gets corrupted, you must reinstall the management server. When you update the Sylink file, the orphaned client reestablishes communication with the management server.
For information on orphaned clients, see:[Update the server certificate on the management server without breaking communications with the client](#)

Methods for replacing the client-server communications file on the client computer

To replace the client-server communications file (Sylink.xml) on the client computer, you can use one of the following methods:

- Redeploy a client installation package on the client computer. Use this method if manually importing the Sylink.xml in a large environment is physically not possible and it requires administrative access. See:
[Restoring client-server communications with Communication Update Package Deployment](#)
- Write a script that runs the SylinkDrop tool.
Use SylinkDrop for many clients or if you use a software management tool to download the client software to computers. The advantage of the software management tool is that it downloads the Sylink.xml file when the client user turns on the client computer. In comparison, the client installation package downloads the new Sylink.xml file only after the client computer connects to the management server. See:
[Restoring client-server communication settings by using the SylinkDrop tool](#)
- Export the Sylink.xml file to the client computer using the **Export Communication Settings** command and importing it on the client computer manually. You should use this method if you want to use a software management tool. With a software management tool, the job is queued up and completed whenever the users turn on their computers. With the other methods, the client computer must be online. See:
[Exporting the client-server communications file \(Sylink.xml\) manually](#)
- Export the Sylink.xml file to the client computer using the **Export Communication Settings** command and import it on the client computer manually using the following command: `smc -importsylink <sylinkpath>` See:
[Exporting the client-server communications file \(Sylink.xml\) manually](#)

Regardless of which method you use, the client immediately connects to the management server. The management server places the client in the group that is specified in the communications file. The client is updated with the policies and settings of the group. After the client and the management server communicate, the notification area icon with the green dot appears in the client computer taskbar. See:

[Checking whether the client is connected to the management server and is protected](#)

More information

- [Client and server communication files](#)
- [How does the client computer and the management server communicate?](#)

Restoring client-server communication settings with the SylinkDrop tool

The Sylink.xml file includes communication settings between the client and a Symantec Endpoint Protection Manager server. If the clients have lost the communication with a management server, you must replace the old Sylink.xml file with a new Sylink.xml file. The SylinkDrop tool automatically replaces the Sylink.xml file on the Windows client computer with a new Sylink.xml file.

For information on other methods to replace the client computer, see: [Replacing the client-server communications file on the client computer](#)

When you replace the existing Sylink file, it can also perform the following tasks:

- Migrates or moves clients to a new domain or management server.
- Restores the communication breakages to the client that cannot be corrected on the management server.
- Moves a client from one server to another server that is not a replication partner.
- Moves a client from one domain to another.
- Converts an unmanaged client to a managed client.

On the management server, you can find the SylinkDrop tool at `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools\SylinkDrop`.

. You can run the tool remotely or can save it and then run it on the client computer. In 14.3 RU4 and earlier, the SylinkDrop tool was installed on the client computer.

To restore client-server communication settings with the SylinkDrop tool

1. In the management console, export the communications file from the group that connects to the management server to which you want the client computer to connect. The communications file is the Sylink.xml file. See: [Exporting the client-server communications file \(Sylink.xml\) manually](#)
2. Copy the Sylink.xml file to the client computer.
You can either save the file to a network location, email it to the user on the client computer, or copy it to removable media.
3. Open the SylinkDrop tool, and click **Browse** to locate the .xml file you deployed in step 2 to the client computer.
4. Click **Update Sylink**.
5. When you see a confirmation dialog box, click **OK**.
6. In the **Sylink Drop** dialog box, click **Exit**.

Restoring client-server communications with Communication Update Package Deployment

If the client-server communications break, you can quickly restore communications by replacing the Sylink.xml file on the client computer. You can replace the Sylink.xml file by deploying a communication update package. Use this method for a large number of computers, for the computers that you cannot physically access easily, or the computers that require administrative access.

For more information, see:

-
- [How does the client computer and the management server communicate?](#)
 - [How do I replace the client-server communications file on the client computer?](#)

To restore client-server communications with Communication Update Package Deployment

1. In the console, launch the **Client Deployment Wizard**.

Click **Help > Getting Started Page** and then under **Required tasks**, click **Install the client software on your computers**.

2. In the **Client Deployment Wizard**, under **Communication Update Package Deployment**, select whether you want a package for Windows or Mac clients, and then click **Next**.

3. Select the group on which you want to apply the policy, and then click **Next**.

For Windows clients only, you can set password protection. See:

[Password-protecting the Symantec Endpoint Protection client](#)

4. Choose one of the following deployment methods, and then click **Next**:

- Click **Remote Push** and go to the **Computer Selection** step in the following procedure. See: [Installing Symantec Endpoint Protection clients with Remote Push](#)
- Click **Save Package** and go to the **Browse** step in the following procedure. See: [Installing Symantec Endpoint Protection clients with Save Package](#)

5. After the communication update package is applied, confirm that the computers successfully communicate with Symantec Endpoint Protection Manager.

More information

- [Checking whether the client is connected to the management server and is protected](#)
- [Running a report on the deployment status of clients](#)

Exporting and importing the client-server communications file (Sylink.xml) manually

If the Windows client and the management server do not communicate, you should replace the Sylink.xml file on the client computer to restore communications. You can manually export the Sylink.xml file from Symantec Endpoint Protection Manager on a group basis.

For more information about other situations when you should replace the communications file, see: [Replacing the client-server communications file on the client computer](#)

Exporting the Sylink.xml file

To export the client-server communications file (Sylink.xml) manually

1. In the console, click **Clients**.
2. Under **Clients**, select the group in which you want the client to appear.
3. Right-click the group, and then click **Export Communication Settings**.
4. In the **Export Communication Settings for group name** dialog box, click **Browse**.
5. In the **Select Export File** dialog box, locate the folder to where you want to export the .xml file, and then click **OK**.
6. Under **Preferred Policy Mode**, make sure that **Computer Mode** is checked.
7. Click **Export**, and then **OK**.

Importing the Sylink.xml file

After you export the sylink file from the Symantec Endpoint Protection Manager, you import it into the client computer.

You can use one of the following methods for importing the sylink.xml file.

To import the client-server communications file using the import sylink command

1. On the client computer, open a command line and type: `smc -importsylink <sylinkpath>` or `smc -importsylink -p <sylinkpath>` where *p* is the password.

To import the client-server communications file using the Troubleshooting menu

1. Open Symantec Endpoint Protection on the computer that you want to replace the sylink.xml file.
2. In the upper right, click **Help**, and then click **Troubleshooting**.
3. In the **Troubleshooting** dialog box, in the **Management** pane under **Communication Settings**, click **Import**.
4. In the **Import Group Registration Settings** dialog box, locate the `<group name>_sylink.xml` file, and then click **Open**.
5. Click **Close** to close the **Troubleshooting** dialog box.

After you import the communications file, and the client and the management server communicate, the notification area icon appears with a green dot in the computer taskbar. The green dot indicates that the client and the management server are in communication with each other.

More information

[Password-protecting the Symantec Endpoint Protection client](#)

Importing client-server communication settings into the Linux client

(For 14.3 MP1 and earlier)

After you install an unmanaged Symantec Endpoint Protection for Linux client, you can convert it to a managed client to centrally manage the client's policies and status with Symantec Endpoint Protection Manager. A managed client communicates with and reports its status and other information to Symantec Endpoint Protection Manager.

You can also use this procedure to reconnect a previously orphaned client with Symantec Endpoint Protection Manager.

NOTE

You must have superuser privileges to perform this procedure. The procedure uses `sudo` to demonstrate this elevation of privilege as required.

The text `path-to-sav` represents the path to the `sav` command. The default path is `/opt/Symantec/symantec_antivirus/`.

To import the client-server communication settings file into the Linux client

1. You or the Symantec Endpoint Protection Manager administrator must first export the communication settings file from Symantec Endpoint Protection Manager and copy it to the Linux computer. Ensure that the file name is `sylink.xml`.

[Exporting the client-server communications file \(Sylink.xml\) manually](#)

2. On the Linux computer, open a terminal window and enter the following command:

```
sudo path-to-sav/sav manage -i path-to-sylink/sylink.xml
```

Where `path-to-sylink` represents the path to which you copied `sylink.xml`.

For example, if you copied it to your user profile's desktop, enter:

```
sudo path-to-sav/sav manage -i ~/Desktop/sylink.xml
```

3. A successful import returns OK. To further verify the managed status, enter the following command, which displays the policy serial number for a successful import:

```
path-to-sav/sav manage -p
```

For more information, see:

[Installing the Symantec Endpoint Protection client for Linux](#)

NOTE

As of Linux client 14.3 RU2, you can use the **sav** command to import the *sylink.xml* file. See:

[Running the Linux client command line tool \(sav\)](#).

IPv6 networking support

This support was added in version 14.2.

IPv6 is a revision to the Internet Protocol that is a successor of IPv4. Both types of addresses provide the unique, numerical IP addresses necessary for Internet-enabled devices to communicate. IPv4 addresses are 32-bit, and IPv6 addresses are 128-bit. Therefore, IPv6 allows for more addresses to be available for users and devices to communicate on the Internet.

IPv6 addresses are conventionally expressed using hexadecimal strings. For example, `fd32:32a4:d0cf:a0c4:0000:8a2e:0370:7334`, which can also be expressed as `fd32:32a4:d0cf:a0c4::8a2e:0370:7334`. When you enter an IPv6 address that ends in a port number, you must enclose the IPv6 address in square brackets. The brackets keep the port number from being interpreted as part of the IPv6 address. For example: `http://[fd32:32a4:d0cf:a0c4::8a2e:0370:7334]:9090`.

Symantec Endpoint Protection 14.2 supports IPv6 in the following ways:

- Communication between the management server and Windows, Mac, and Linux clients.
- Communication between the console and the management server, such as logging on locally or remotely to Symantec Endpoint Protection Manager. See:
[Logging on to the Symantec Endpoint Protection Manager console](#)
- Communication between management servers and internal LiveUpdate servers that run LiveUpdate Administrator. See:
[Configuring clients to download content from an internal LiveUpdate server](#)
- Windows LiveUpdate to management server.
- Communication between management server or clients and services or functions like LiveUpdate Engine (LUE) and reputation look-ups.
- Definition of locations in Location Awareness with IPv6-based criteria.

Furthermore, many other policies now let you enter IPv6 addresses as defining criteria in addition to IPv4, such as custom IPS signatures or explicit GUPs.

IPv6 is not supported for the following items:

- Two-factor authentication (2FA) with Symantec VIP. See:
[Configuring two-factor authentication with Symantec VIP](#)
- Enrolling with and connecting to the cloud console.

Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients

Symantec Endpoint Protection Manager uses an Apache web server to communicate with clients and provide reporting services. For new installations of Symantec Endpoint Protection, HTTPS communications are enabled by default. HTTPS is a secure protocol that uses a certificate to sign and encrypt data, which provides for the confidentiality and the integrity of the communications.

If you upgraded directly from a 12.1.x version, or HTTPS communications was disabled, you should enable HTTPS.

Table 141: Configuring HTTPS communication to the client

Step	Description
Step 1: Check that the default HTTPS port is available	By default, HTTPS traffic uses port 443. In some networks, port 443 may already be bound to another application or service. Before you enable HTTPS communication, you must check to see if the default port is available. See: Verifying port availability
Step 2: Change the default HTTPS port as needed	If port 443 is not available, choose an unused port from the high port range (49152-65535). Configure the management server to use the new port. Update the management server list to reflect the new port. See: • Changing the HTTPS port for Apache for client communication • Configuring a management server list for load balancing
Step 3: Enable HTTPS communication to the client	Edit the Apache httpd.conf file to allow HTTPS communication to the client. Test the connection, and then switch the clients to HTTPS communication. See: Enabling HTTPS client-server communications

More information

[Managing the client-server connection](#)

Finding an available port

Some Symantec Endpoint Protection Manager configurations require that you change a default port assignment to prevent a conflict with other applications or services. Before you assign a new port, you must check to be sure that another application or service does not use the new port.

Open a command prompt and enter the following case-sensitive command:

```
netstat -an | find ":port" | find "LISTENING"
```

Where port represents the port number for which you want to check availability. For example, to see if port 443 is available, enter:

```
netstat -an | find ":443" | find "LISTENING"
```

If the `netstat` command returns a result, you must find an unused port. You use the same command, but replace `port` with the port of your choice. If this command yields no results, then the port is free to use.

More information

- [Changing the HTTPS port for Apache for client communication](#)
- [Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients](#)

Changing the HTTPS port for Apache for client communication

The default HTTPS port for Apache is port 443. If the system hosting Symantec Endpoint Protection Manager also hosts other HTTPS services, port 443 may already be assigned. You should use a different port for new installations to minimize conflict with any applications that already use the default port 443. If you want clients to use the default port to communicate with Symantec Endpoint Protection Manager, you should first verify that port is available.

NOTE

If you customize the HTTPS port number after you deploy the client software, the clients lose communication with the management server. They reestablish communication after the next client update from the server, which contains the new connection information. You can also use a Communication Update Package. See:

[Restoring client-server communications with Communication Update Package Deployment](#)

After you complete this procedure, you enable HTTPS client-server communications.

To change the HTTPS port for Apache for client communication

1. In a text editor, open the following file:

`SEPM_Install\apache\conf\ssl\sslForClients.conf`

SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

NOTE

The enclosing folder `SEPM_Install\apache\conf\ssl\` may be read-only. In that case, you may need to uncheck **Read-only** in the folder properties.

2. Edit the following lines and replace the default of 443 with the new port number:

`Listen 443`

`<VirtualHost_default_: 443>`

3. Save the file and close the text editor.

More information

- [Enabling HTTPS client-server communications](#)
- [Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients](#)

Enabling HTTPS client-server communications

You edit the `httpd.conf` file to enable secure communication between the Symantec Endpoint Protection Manager server and the clients using the HTTPS protocol.

If you need to use an alternate port for secure communication, you must change the port assignment in Symantec Endpoint Protection Manager first.

For new installations of Symantec Endpoint Protection, HTTPS client-server communications is enabled by default.

To enable HTTPS for the Apache web server

1. In a text editor, open the following file:

`SEPM_Install\apache\conf\httpd.conf`

SEPM_Install by default is C:\Program Files\Symantec\Symantec Endpoint Protection Manager.

2. Find the following text string and remove the hash mark (#):

`#Include conf/ssl/sslForClients.conf`

3. Save and then close the file.

4. Restart the **Symantec Endpoint Protection Manager Webserver** service.

Stopping and restarting the Symantec Endpoint Protection Manager Webserver service also stops and restarts the Symantec Endpoint Protection Manager service.

[Stopping and starting the Apache Web server](#)

To verify HTTPS works correctly

1. Enter the following URL in a web browser:

`https://SEPMServer:port/secars/secars.dll?hello,secars`

Where `SEPMServer` is the server host name for Symantec Endpoint Protection Manager and `port` is the HTTPS port number. By default, HTTPS traffic uses port 443.

2. If the browser displays the word **OK**, the HTTPS connection is successful.

If a page error displays, repeat the previous steps and check that you formatted all strings correctly. Also check that you entered the URL correctly.

If you did not update the management server with a certificate authority-signed certificate and private key pair, the web browser displays a warning that the certificate is not trusted. The same warning appears when you access the website from a URL that is different than the subject name on the management server certificate, which is expected.

To switch the clients to use HTTPS for communication with Symantec Endpoint Protection Manager

1. In the Symantec Endpoint Protection Manager console, on the **Policies** tab, click **Policy Components > Management Server Lists**.
2. Double-click the management server list that your client groups and locations use. If you only have the default management server list, duplicate it, and then double-click the new list to edit it.
You can also click **Add a Management Server List**, under **Tasks**. Add the server information under **Management Servers, Add > New Server**. You can add one **New Server** entry for server IP address, and one for server name.
[Copying and pasting a policy on the Policies page](#)
3. Click **Use HTTPS protocol**.
Only click **Verify certificate when using HTTPS protocol** if you have previously updated the management server with a Certificate Authority-signed certificate and a private key pair.

[Best practices for updating server certificates and maintaining the client-server connection](#)

NOTE

If you used a custom HTTPS port number in the `sslForClients.conf` file, edit the server from the list of management servers. Click **Customize HTTPS port**, and then edit the port to match the number you previously used.

Click **OK** to save the custom port.

4. Click **OK** to save your management server list.
5. If you edited a copy of the default management server list, right-click it, click **Assign**, and then assign it to every group and location.

[Assigning a management server list to a group and location](#)

As the clients receive the updated management server list, the clients switch to HTTPS for communication with Symantec Endpoint Protection Manager.

NOTE

You should wait at least 24 hours for the changes to complete. Waiting up to one week is recommended, which allows as many clients as possible to download the new communication details from the management server. Users who are out of the office or on leave may not receive these updates on their device because it is offline. Many institutions run the failover method for 30 days or more to catch as many out-of-office clients as possible.

To confirm client communication to the management server

1. On the Symantec Endpoint Protection client, click **Help > Troubleshooting > Server Connection Status**.
2. Under **Last Attempted Connection** and **Last Successful Connection**, confirm the display of both the server address and the port number for HTTPS communications.
3. Click **Connect Now** to force an immediate connection, if desired.

More information

- [Changing the HTTPS port for Apache for client communication](#)
- [Setting up HTTPS communications between a Symantec Endpoint Protection Manager and the clients](#)

Managing Groups, Clients, Administrators, Passwords, and Domains

Learn how to add and manage groups, clients, administrators, passwords, and domains.

This section describes how to manage groups of client computers, clients, administrators, passwords, and domains.

Managing groups of clients

In Symantec Endpoint Protection Manager, groups function as containers for the endpoints that run the client software. These endpoints can be either computers, or users. You organize the clients that have similar security needs into groups to make it easier to manage network security.

Symantec Endpoint Protection Manager contains the following default groups:

- The **My Company** group is the top-level, or parent, group. It contains a flat tree of child groups.
- The **Default Group** is a subgroup of **My Company**. Clients are first assigned to the **Default Group** when they first register with Symantec Endpoint Protection Manager, unless they belong to a predefined group. You cannot create subgroups under the **Default Group**.

NOTE

You cannot rename or delete **My Company** or **Default Group** in either Symantec Endpoint Protection Manager or the cloud console.

Table 142: Group management actions

Task	Description
Add groups	For more information, see: How you can structure groups Adding a group
Import existing groups	If your organization already has an existing group structure, you can import the groups as organizational units. Note: You cannot manage imported organizational units in the same ways that you can manage the groups that you create in Symantec Endpoint Protection Manager. For more information, see: Importing existing groups and computers from an Active Directory or an LDAP server
Disable inheritance for subgroups	The subgroups inherit the same security settings from the parent group by default. You can disable inheritance. See: Disabling a group's inheritance
Create locations within groups	You can set up the clients to switch automatically to a different security policy if the physical location of the client changes. See: Managing locations for remote clients Some security settings are group-specific and some settings are location-specific. You can customize any settings that are location-specific. See: Configuring communication settings for a location

Task	Description
Manage security policies for groups	You can create security policies based on the needs of each group. You can then assign different policies to different groups or locations. See: • Adding a policy • Assigning a policy to a group or location • Performing the tasks that are common to all policies
Perform group maintenance	You can move groups for easier management and move clients between groups. You can also block clients from being added to a particular group. See: • Moving a client computer to another group • Blocking client computers from being added to groups

How you can structure groups

You can create multiple groups and subgroups to match the organizational structure and security of your company. You can base your group structure on function, role, geography, or a combination of criteria.

Table 143: Criteria for creating groups

Criterion	Description
Function	You can create groups based on the types of computers to be managed, such as laptops, desktops, and servers. Alternatively, you can create multiple groups that are based on usage type. For example, you can create a remote group for the client computers that travel and a local group for the client computers that remain in the office.
Role	You can create groups for department roles, such sales, engineering, finance, and marketing.
Geography	You can create groups based on the offices, cities, states, regions, or countries where the computers are located.
Combination	You can create groups based on a combination of criteria. For example, you can use the function and the role. You can add a parent group by role and add child subgroups by function, as in the following scenario: • Sales, with subgroups of laptops, desktops, and servers. • Engineering, with subgroups of laptops, desktops, and servers.

After you organize the client computers into groups, you can apply the appropriate amount of security to that group.

For example, suppose that a company has telemarketing and accounting departments. These departments have staff in the company's New York, London, and Frankfurt offices. All computers in both departments are assigned to the same group so that they receive virus and security risk definitions updates from the same source. However, IT reports indicate that the telemarketing department is more vulnerable to risks than the accounting department. As a result, the system administrator creates separate telemarketing and accounting groups. Telemarketing clients share configuration settings that strictly limit how users can interact with their virus and security risk protection.

For more information, see:

- [Best Practices for Creating Group Structure](#)
- [Performing the tasks that are common to all policies](#)
- [Managing groups of clients](#)

Adding a group

You can add groups after you define the group structure for your organization.

Group descriptions may be up to 1024 characters long. Group names may contain any character except the following characters: " / \ * ? < > | : Group descriptions are not restricted.

NOTE

You cannot add groups to the Default Group.

For more information, see:

[How you can structure groups](#)

To add a group

1. In the console, click **Clients**.
2. Under **Clients**, select the group to which you want to add a new subgroup.
3. On the **Clients** tab, under **Tasks**, click **Add Group**.
4. In the **Add Group for group name** dialog box, type the group name and a description.
5. Click **OK**.

Synchronizing Active Directory groups with the Symantec Endpoint Protection Manager (SEPM)

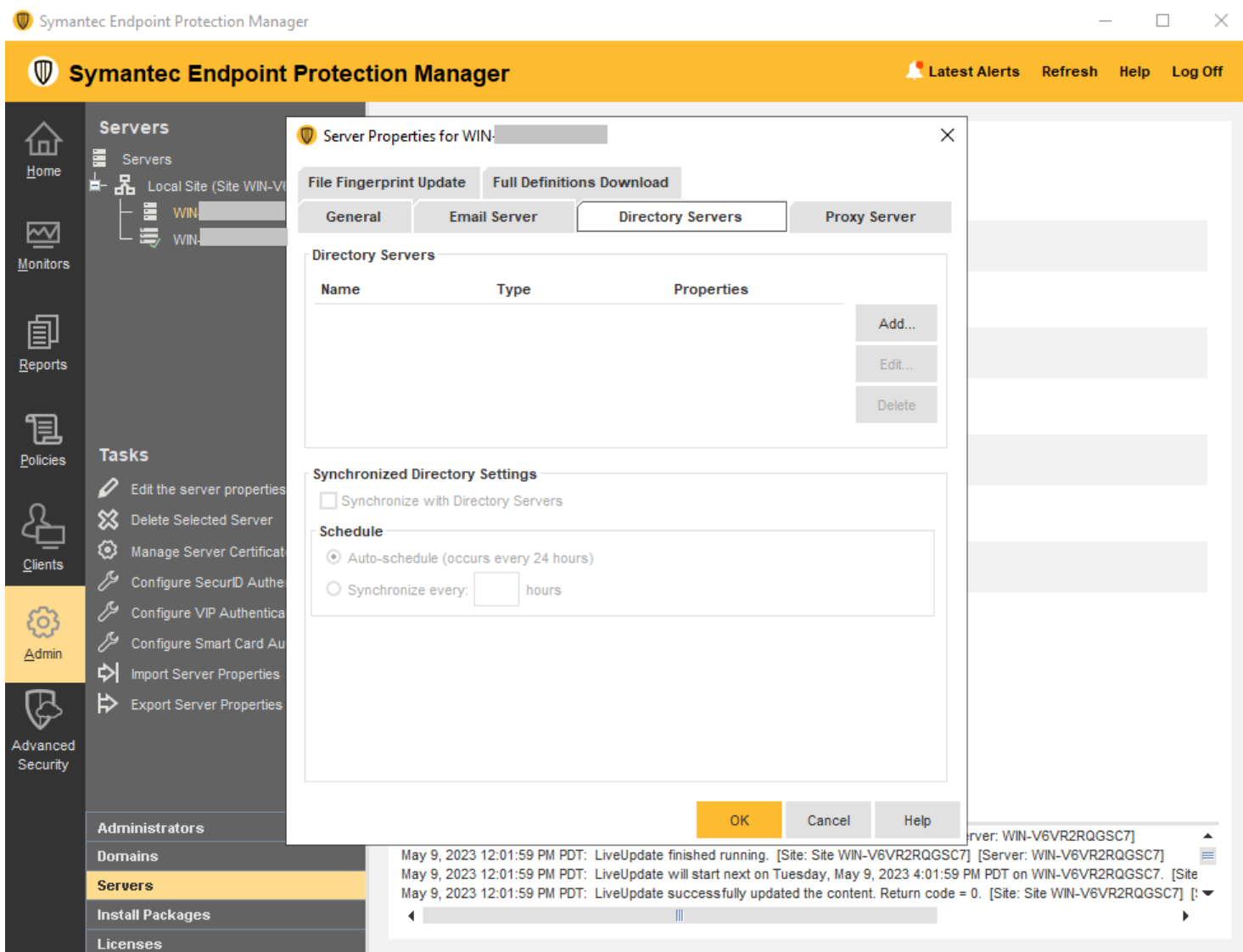
If your company uses either Active Directory (AD) or an LDAP server to manage groups, you can import the group structure into Symantec Endpoint Protection Manager. You then manage the groups and computers from the management console.

NOTE

Do not synchronize the Active Directory groups with more than one Symantec Endpoint Protection Manager.

Step 1: Integrate the Active Directory with the Symantec Endpoint Protection Manager (SEPM)

1. In the console, click **Admin > Servers**.
2. Under **Servers > Local Site**, right-click the management server and click **Edit the server properties**.
3. In the **Server Properties** dialog box, on the **Directory Servers** tab, click **Add**.



4. In the **Add Directory Server** dialog box, type the domain name for the directory server.
5. Click **Active Directory**.
Enter the username and password for a domain user or a dedicated service account.
If you add an LDAP server, change the port number of the LDAP server if it should be different from the default value.
6. In the **Server IP Address or Name** field, enter your company IP address or domain name. For example, for an email address of `abc@mycompany.com`, add the domain name: `mycompany.com`.
7. Click **OK**.
If you did not successfully verify the credentials, check **Use Secure Connection** and click **OK**.
Use Secure Connection uses LDAP 636, and provides an encrypted connection.

Server Properties for WIN-

×

File Fingerprint Update

Full Definitions Download

General

Email Server

Directory Servers

Proxy Server

Directory Servers

Name	Type	Properties	
DDC2016	Active Directory	Server:DC2016, User:do...	Add... Edit... Delete

Synchronized Directory Settings

☒ Synchronize with Directory Servers

Schedule

☒ Auto-schedule (occurs every 24 hours)

☐ Synchronize every: hours

OK

Cancel

Help

9. Click **OK**.

Step 2: Import the Active Directory organizational units

You can import the organizational unit as a subgroup of either the **My Company** group or a group you create, but not the **Default Group**. You cannot create groups as a subgroup of an organizational unit. You cannot place an organizational unit in more than one Symantec Endpoint Protection Manager group.

NOTE

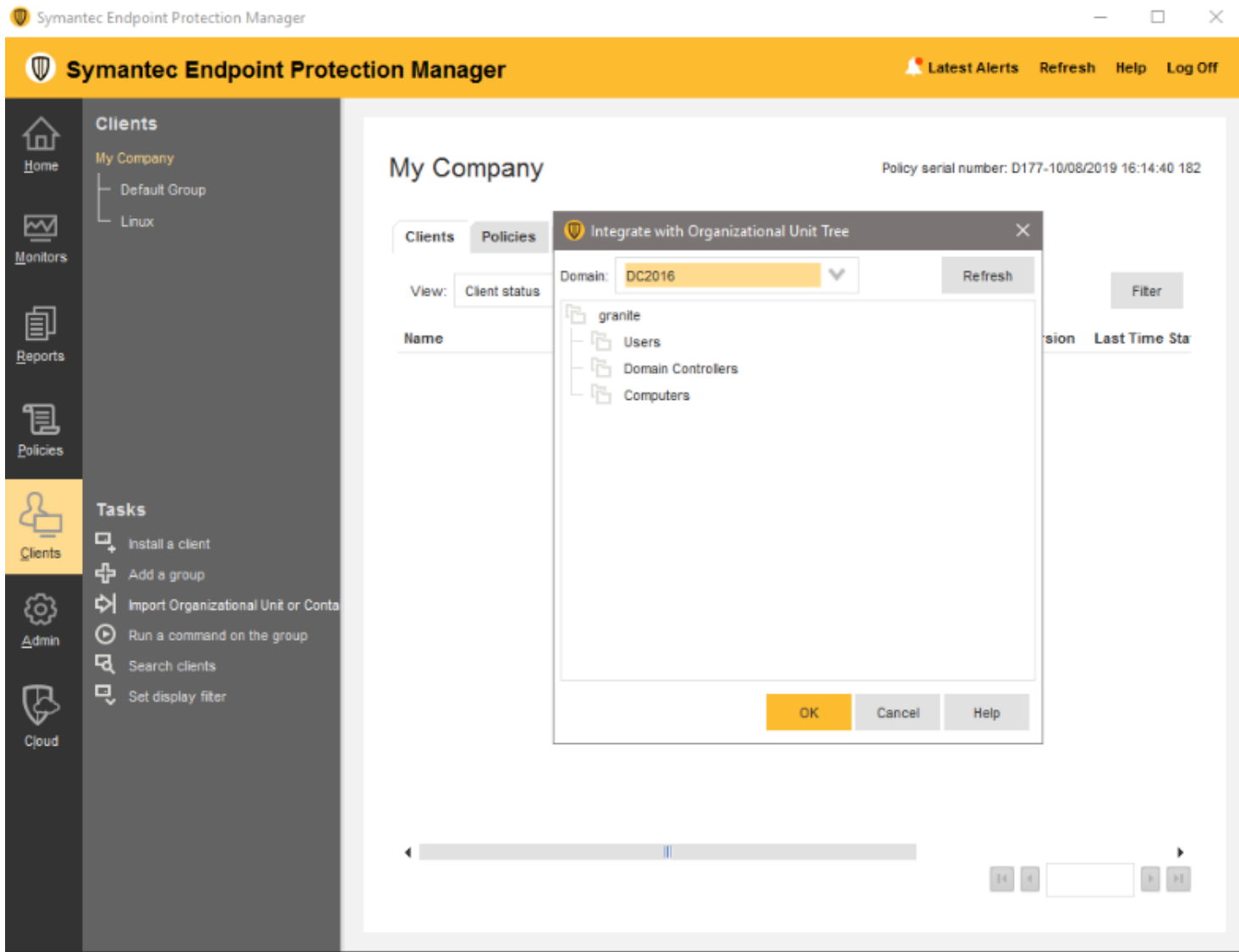
Before you import organizational units into Symantec Endpoint Protection Manager, you must convert some of the special characters that precede a computer name or user name. You perform this task in the directory server. You must convert special characters so that the management server imports these accounts.

Convert the following special characters:

- A space or a hash character (#) that occurs at the beginning of an entry.
- A space character that occurs at the end of an entry.
- A comma (,), plus sign (+), double quotation mark ("), less than or greater than symbols (< or >), equals sign (=), semi-colon (;), backslash (\).

To allow a name that includes these characters to be imported, you must precede each character with a backslash character (\).

1. On the **Clients** page > **Clients** tab, select the group to which you want to add the Active Directory organizational units.
2. Under **Tasks**, click **Import Organizational Unit or Container**.
3. In the **Domain** drop-down list, select the domain name that you created in the previous step.
4. Click **OK**.



5. Select the appropriate OU to integrate with the management server and click **OK**.

See: [What are organizational units in Active Directory?](#)

Troubleshooting synchronization issues

For issues with AD synchronization, check the following logs.

- 32-bit: C:\Program Files\Symantec\Symantec Endpoint Protection Manager\Tomcat\logs\ADSI\Task-0.log
- 64-bit: C:\Program Files(x86)\Symantec\Symantec Endpoint Protection Manager\Tomcat\logs\ADSI\Task-0.log

Search for "Error Code" and next few lines for the cause of the problem.

What are organizational units in Active Directory?

Microsoft Active Directory and LDAP servers use organizational units to manage accounts for computers and users. You can import an organizational unit and its account data into Symantec Endpoint Protection Manager, and manage the

account data in the management console. Because Symantec Endpoint Protection Manager treats the organizational unit as a group, you can then assign a security policy to the organizational unit group.

You can also move accounts from the organizational units into a Symantec Endpoint Protection Manager group by copying the accounts. The same account then exists in both the Symantec Endpoint Protection Manager group and the organizational unit. Because the priority of the Symantec Endpoint Protection Manager group is higher than the organizational unit, the copied accounts adopt the policy of the Symantec Endpoint Protection Manager group.

If you delete an account from the directory server that you copied to a Symantec Endpoint Protection Manager group, the account name still remains in the Symantec Endpoint Protection Manager group. You must remove the account from the management server manually.

If you need to modify the account data in the organizational unit, you perform this task on the directory server, and not in Symantec Endpoint Protection Manager. For example, you can delete an organizational unit from the management server, which does not permanently delete the organizational unit in the directory server. You must synchronize Symantec Endpoint Protection Manager with the Active Directory server so that these changes get automatically updated in Symantec Endpoint Protection Manager. You enable synchronization when you set up the connection to the directory server.

NOTE

Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

You can also import selected users to a Symantec Endpoint Protection Manager group rather than importing the entire organizational unit.

More information

- [Connecting Symantec Endpoint Protection Manager to a directory server](#)
- [Importing existing groups and computers from an Active Directory or an LDAP server](#)
- [Importing organizational units from a directory server](#)

Connecting Symantec Endpoint Protection Manager to a directory server

You must first connect Symantec Endpoint Protection Manager to your company's directory server before you can import the organizational units that contain computer accounts or user accounts.

You cannot modify the accounts in organizational units in the management server, only in the directory server. However, you can synchronize the account data between an Active Directory server and the management server. Any changes you make in the Active Directory server are automatically updated in Symantec Endpoint Protection Manager. Any changes that you make on the Active Directory server do not appear immediately in the organizational unit that was imported into the management server. The latency period depends on the synchronization frequency. You enable synchronization and set the synchronization frequency when you configure the connection.

If you delete a directory server connection from Symantec Endpoint Protection Manager, you must first delete any organizational units that you imported that are associated with that connection. Then you can synchronize data between the servers.

NOTE

Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

To connect Symantec Endpoint Protection Manager to a directory server

-
1. In the console, click **Admin > Servers**.
 2. Under **Servers** and **Local Site**, select the management server.
 3. Under **Tasks**, click **Edit the server properties**.
 4. In the **Server Properties** dialog box, on the **Directory Servers** tab, click **Add**.
 5. In the **Add Directory Server** dialog box, type a name for the directory server.
 6. Check **Active Directory** or **LDAP** and type the IP address, host name, or domain name.
If you add an LDAP server, change the port number of the LDAP server if it should be different than the default value.
 7. If you want an encrypted connection, check **Use Secure Connection**.
 8. Click **OK**.
 9. On the **Directory Servers** tab, check **Synchronize with Directory Servers** and under **Schedule**, set up the synchronization schedule.
 10. Click **OK**.

More information

[Importing organizational units from a directory server](#)

Connecting to a directory server on a replicated site

If a site uses a replicated Active Directory or LDAP server, you can connect Symantec Endpoint Protection Manager to both the primary directory server and the replicated server. If the primary directory server gets disconnected, the management server stays connected to the replicated directory server.

Symantec Endpoint Protection Manager can then authenticate administrator accounts and synchronize organizational units on all the Active Directory servers of the local site and the replicated sites. See:

[Setting up sites and replication](#)

NOTE

Synchronization is only possible for Active Directory Servers. Symantec Endpoint Protection does not support synchronization with LDAP servers.

To connect to a directory server on a replicated site

1. In the console, click **Admin > Servers**.
2. Under **Servers**, select the management server.
3. Under **Tasks**, click **Edit the server properties**.
4. In the **Server Properties** dialog box, on the **Directory Servers** tab, click **Add**.
5. In the **Add Directory Server** dialog box, on the **Replication Servers** tab, click **Add**.
6. In the **Add Replication Server** dialog box, type the IP address, host name, or domain name for the directory server, and then click **OK**.
7. Click **OK**.
8. Click **OK**.

More information

[Connecting Symantec Endpoint Protection Manager to a directory server](#)

Importing organizational units from a directory server

When you import computer accounts or user accounts from an Active Directory or LDAP server, you import these accounts as organizational units. You can then apply a security policy to the organizational unit. You can also copy these accounts to an existing Symantec Endpoint Protection Manager group.

You can import the organizational unit as a subgroup of either the **My Company** group or a group you create, but not the **Default Group**. You cannot create groups as a subgroup of an organizational unit. You cannot place an organizational unit in more than one Symantec Endpoint Protection Manager group.

If you do not want to add all accounts within an organizational unit or container to Symantec Endpoint Protection Manager, then you must still import it. Once the import completes, you copy the accounts that you want to manage to existing client groups.

NOTE

Before you import organizational units into Symantec Endpoint Protection Manager, you must convert some of the special characters that precede a computer name or user name. You perform this task in the directory server. If you do not convert special characters, the management server does not import these accounts.

You must convert the following special characters:

- A space or a hash character (#) that occurs at the beginning of an entry.
- A space character that occurs at the end of an entry.
- A comma (,), plus sign (+), double quotation mark ("), less than or greater than symbols (< or >), equals sign (=), semi-colon (;), backslash (\).

To allow a name that includes these characters to be imported, you must precede each character with a backslash character (\).

To import organizational units from a directory server

1. Connect Symantec Endpoint Protection Manager to a directory server. See:
[Synchronizing Active Directory groups with the Symantec Endpoint Protection Manager \(SEPM\)](#)
2. In the console, click **Clients**, and under **Clients**, select the group to which you want to add the organizational unit.
3. Under **Tasks**, click **Import Organizational Unit or Container**.
4. In the **Domain** drop-down list, choose the directory server name you created in step 1.
5. Select either the domain or a subgroup.
6. Click **OK**.

[What are organizational units in Active Directory?](#)

Disabling a group's inheritance

In the group structure, subgroups initially and automatically inherit the locations, policies, and settings from their parent group. By default, inheritance is enabled for every group. You can disable inheritance so that you can configure separate security settings for a subgroup. If you make changes and later enable inheritance, any changes that you made in the subgroup's settings are overwritten.

Policies that come from the cloud do not follow the Symantec Endpoint Protection Manager policy inheritance configuration. Instead, they follow the inheritance rules that are defined in the cloud. See:

[Managing groups of clients](#)

To disable a group's inheritance

-
1. In the console, click **Clients**.
 2. On the **Clients** page, under **Clients**, select the group for which you want to disable or enable inheritance.
You can select any group except the top-level group, My Company.
 3. In the **group name** pane, on the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.

Blocking client computers from being added to groups

You can set up client installation packages with their group membership already defined. If you define a group in the package, the client computer automatically is added to the appropriate group. The client is added the first time it makes a connection to the management server. See:

Managing client installation packages

You can block a client if you do not want clients to be added automatically to a specific group when they connect to the network. You can block a new client from being added to the group to which they were assigned in the client installation package. In this case, the client gets added to the default group. You can manually move a computer to a blocked group.

To block client computers from being added to groups

1. In the console, click **Clients**.
2. Under **Clients**, right-click a group, and click **Properties**.
3. On the **Details** tab, under **Tasks**, click **Edit Group Properties**.
4. In the **Group Properties for group name** dialog box, click **Block New Clients**.
5. Click **OK**.

More information

Moving a client computer to another group

Moving a client computer to another group

If your client computers are not in the correct group, you can move them to another group.

You can use the following methods:

- The **Move** command on the **Clients** page.
- Redeploy the client installation package.
See: [Restoring client-server communications with Communication Update Package Deployment](#)
- The REST API command (/api/v1/computers).
See: <https://apidocs.securitycloud.symantec.com/#/doc?id=computers>

To move a client computer to another group using the Move command

1. In the console, click **Clients > Clients**, and select a group.
2. On the **Clients** tab with the group selected, select the computer, and then right-click **Move**.
Use the Shift key or the Ctrl key to select multiple computers.

3. In the **Move Clients** dialog box, select the new group.
4. Click **OK**.

Managing client computers

Table 144: Tasks to manage client computers

Task	Description
Check that the client software is installed on your computers	- You can display the computers in each group that do not have the client software installed yet. See: Searching for the clients that do not have the client software installed - You can configure a client computer to detect that other devices do not have the client software installed. Some of these devices might be unprotected computers. You can then install the client software on these computers. See: Configuring a client to detect unmanaged devices - You can add a client to a group and install the client software later. For more information, see: Choosing a method to install the client using the Client Deployment Wizard
Check whether the client is connected to the management server	You can check the client status icons in the management console and in the client. The status icon shows whether the client and the server communicate. See: Checking whether the client is connected to the management server and is protected Symantec Endpoint Protection client status icons A computer may have the client software installed, but is an unmanaged client. You cannot manage an unmanaged client. Instead, you can convert the unmanaged client to a managed client. See: How does the client computer and the management server communicate?
Configure the connection between the client and the server	After you install the client software client computers automatically connect to the management server at the next heartbeat. You can change how the server communicates with the client computer. See: Managing the client-server connection You can troubleshoot any connection issues. See: Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the database
Check that client computers have the right level of protection	- You can view the status of each protection technology on your client computers. See: Viewing the protection status of client computers Checking whether the client is connected to the management server and is protected - You can run reports or view logs to see whether you need to increase protection or improve performance. For example, the scans may cause false positives. You can also identify the client computers that need protection. See: Monitoring the Symantec Endpoint Protection clients - You can modify protection based on specific attributes of the client software or the client computers. See: Searching for information about client computers
Adjust the protection on client computers	If you decide that clients do not have the right level of protection, you can adjust the protection settings. - You can increase or decrease each type of protection based on the results in the reports and logs. See: The types of security policies How Symantec Endpoint Protection technologies protect your computers - You can require a password on the client. See: Password-protecting the Symantec Endpoint Protection client

Task	Description
Move endpoints from one group to another to modify protection (optional)	To change a client computer's level of protection, you can move it to a group that provides more protection or less protection. See: Moving a client computer to another group When you deploy a client installation package, you specify which group the client goes in. You can move the client to a different group. But if the client gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. To keep the client with the group it was last moved to, configure the reconnection preferences. You configure these settings in the Communications Settings dialog box on the Clients > Policies tab. See: Communications Settings for <group_name>
Decide whether users should have control over computer protection (optional)	You can specify the kind of control that users have over the protection on client computers. - For Virus and Spyware Protection, Proactive Threat Protection, and Memory Exploit Mitigation, you can lock or unlock a check box within the policies to specify whether users can change individual settings. - For the Firewall policy and the IPS policy and for some client user interface settings, you can change the user control level more generally. See: Preventing users from disabling protection on client computers - If users need full control of the client, you can install an unmanaged client. See: How does the client computer and the management server communicate?
Remove the Symantec Endpoint Protection client software from decommissioned computers (optional)	If you decommissioned a client computer and you want to use the license for a different computer, you can uninstall the Symantec Endpoint Protection client software. For the managed clients that do not connect, Symantec Endpoint Protection Manager deletes clients from the database after 30 days by default. You can change the period of time after which Symantec Endpoint Protection Manager deletes the client from the database. By deleting a client, you also save space in the database. See: Uninstalling the Symantec Endpoint Protection client for Windows Uninstalling the Symantec Endpoint Protection client for Mac Uninstalling the Symantec Endpoint Protection client for Linux Purging obsolete clients from the database to make more licenses available

Viewing the protection status of client computers

You can view information about the real-time operational and protection status of the clients and the computers in your network, such as:

- A list of managed client computers that do not have the client installed.
You can view the computer name, the domain name, and the name of the user who is logged on.
- Which protections are enabled and disabled.
- Which client computers have the latest policies and definitions.
- The group's policy serial number and the client's version number.
- The information about the client computer's network components, such as the MAC address of the network card that the computer uses.
- The system information about the client computer, such as the amount of available disk space and the operating system version number.

After you know the status of a particular client, you can resolve any security issues on the client computers. You can resolve many issues by running commands on groups. For example, you can update content, or enable Auto-Protect.

NOTE

If you manage any clients that run an earlier version of Symantec Endpoint Protection, some newer protection technologies may be listed as **not reporting**. This behavior is expected. It does not mean that you need to take action on these clients.

For more information, see:

- [Checking whether the client is connected to the management server and is protected](#)
- [Running commands on client computers from the console](#)
- [Searching for the clients that do not have the client software installed](#)

To view the protection status of client computers

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, locate the group that contains the clients that you want information about.
3. On the **Clients** tab, click the **View** drop-down list. Then, select a category.

You can go directly to a particular page by typing the page number in the text box at the bottom right-hand corner.

Enabling protection on the client computer

Symantec Endpoint Protection for Windows Client Guide

You should keep all types of protection enabled on your computer at all times, especially Auto-Protect.

On the client, when any of the protections are disabled:

- The status bar is red at the top of the **Status** page.
- The client's icon appears with a universal no sign, a red circle with a diagonal slash. The client icon appears as a full shield in the taskbar in the lower-right corner of your Windows desktop. In some configurations, the icon does not appear.

[Symantec Endpoint Protection client status icons](#)

On a managed client, your administrator can enable or disable a protection technology at any time. If you disable a protection, your administrator may later enable the protection again. Your administrator might also lock a protection so that you cannot disable it

To enable protection technologies from the Status page	On the client, at the top of the Status page, click Fix or Fix All .
To enable protection technologies from the taskbar	On the Windows desktop, in the notification area, right-click the client icon, and then click Enable Symantec Endpoint Protection .
To enable protection technologies from within the client	In the client, on the Status page, beside the protection type, click Options > Enable the <protection type> .
To enable the firewall	1. On the client, at the top of the Status page, next to Network and Host Exploit Mitigation, click Options > Change Settings. 2. On the Firewall tab, check Enable Firewall. 3. Click OK.

Searching for the clients that do not have the client software installed

You can search for clients in a group based on the following criteria:

- Client software is installed.
- Clients run on Windows, Mac, or Linux computers
- Windows clients are in computer mode or user mode.
- Clients are non-persistent and offline in Virtual desktop infrastructures.

For more information, see:

- [Viewing the protection status of client computers](#)
- [Checking whether the client is connected to the management server and is protected](#)

To search for clients

-
1. In the console, click **Clients**.
 2. In the **Clients** pane, choose the group you want to search on.
 3. On the **Clients** tab, under **Tasks**, click **Set display filter**.
 4. In the **Set Display Filter** dialog box, check **New users or computers that have been created but that don't yet have the client software installed**.
 5. Click **OK**.

Searching for information about client computers in the Symantec Endpoint Protection Manager

You can search for information about the clients, client computers, and users to make informed decisions about the security of your network.

For example, you can find which computers in the Sales group run the latest operating system. You can find out which client computers in the Finance group need the latest virus definitions installed.

NOTE

To search for most of the information about the users, you must collect user information either during the client software installation or later. This user information is also displayed on the General tab and the User Info tab in the client's Edit Properties dialog box.

For more information, see:

[Collecting user information](#)

To search for information about client computers in the Symantec Endpoint Protection Manager

1. In the console, click **Clients**.
2. Under **Tasks**, click **Search clients**.
3. In the **Search clients** dialog box, in the **Find** drop-down list, click either **Computers** or **Users**.
4. Click **Browse** to select a group other than the default group. Click to select the group, and then click **OK**.
5. Under **Search Criteria**, click in the **Search Field** to see the drop-down list, and then select the criteria by which you want to search.

To find embedded clients, you can search for the type of write filters in use. Click **Enhanced Write Filter**, **File Based Write Filter**, or **Unified Write Filter** to search for whether they are installed, enabled, or both. You can also search for the reduced-size client. Click **Install Type** to search for a value of **Reduced Size**.

6. Click the **Comparison Operator** drop-down list, and then select a comparison operator.

You can use standard Boolean operators in your search criteria. Click **Help** for more information on the options.

7. In the **Value** cell, type the search string.
8. Click **Search**.

You can export the results into a text file.

9. Click **Close**.

You can export the data that is contained in the query into a text file. See:

[Viewing the protection status of client computers](#)

What are the commands that you can run on client computers?

You can run commands remotely on individual clients or an entire group from the console.

To see the results of any of the commands, click **Monitors** page > **Logs** > **Command Status**. You can also run some of the commands from the **of type** drop-down list.

System administrators and domain administrators can run these commands automatically. For limited administrators, you enable or disable access for each command individually. See:

- [Adding an administrator account and setting access rights](#)
- [Running commands on client computers from the console](#)

Table 145: Commands that you can run on client computers

Commands	Description
Analyze (Removed in 14.3)	In earlier releases, the Analyze command showed the progress of all requests that you submitted for analysis from the cloud console to the Content Analysis System (CAS).
Cancel Evidence of Compromise Scan	Starts or cancels a scan that you use on third-party remote monitoring and management.
Scan	Runs an on-demand scan on the client computers. If you run a scan command, and select a Custom scan, the scan uses the command scan settings that you configured on the Administrator-defined Scans page. The command uses the settings that are in the Virus and Spyware Protection policy that is applied to the selected client computers. See: Running on-demand scans on client computers Note: You can run only a custom scan on Mac client computers.
Update Content	Updates content on clients by initiating a LiveUpdate session on the client computers. The clients receive the latest content from Symantec LiveUpdate. See: Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager
Update Content and Scan	Updates content by initiating a LiveUpdate session and runs an on-demand scan on client computers.
Start Power Eraser Analysis	Runs a Power Eraser analysis on the selected computers. You should typically run Power Eraser only on a single computer or a small number of computers. You should only run Power Eraser when computers exhibit instability or have persistent problems. Unlike other scans, Power Eraser does not automatically remediate any potential threats. You must review the detections in the logs and specify which risks you want to remove or leave alone. Note: Mac and Linux client computers do not process this command. For more information, see: Starting Power Eraser analysis from Symantec Endpoint Protection Manager
Restart Client Computers	Restarts the client computers. If users are logged on to the client, they are warned based on the restart options that the administrator has configured for that client. You can configure client restart options on the General Settings page. Note: Restart options apply only to Windows client computers. Mac client computers always perform a hard restart. Linux client computers ignore this command. For more information, see: Restarting the client computers from Symantec Endpoint Protection Manager Note: You can ensure that a Windows client does not restart. You can add a registry key on the client that keeps it from restarting even if an administrator issues a restart command. See: Ensuring that a client does not restart Note: Ensuring that a client does not restart

Commands	Description
Enable Auto-Protect	Enables Auto-Protect for the file system on the client computers. By default, Auto-Protect for the file system is enabled. Symantec recommends that you always keep Auto-Protect enabled. You can lock the setting so that users on client computers cannot disable Auto-Protect. See: • Customizing Auto-Protect for Windows clients • Customizing Auto-Protect for Mac clients If Auto-Protect for email is disabled, you enable it in the Virus and Spyware Protection policy.
Enable Network Threat Protection and Disable Network Threat Protection	Enables or disables the firewall and enables intrusion prevention on the client computers. Note: Linux client computers do not process this command. For more information, see: Managing firewall protection
Enable Download Insight and Disable Download Insight	Enables or disables Download Insight on the client computers. Note: Mac and Linux client computers do not process this command. For more information, see: Managing Download Insight detections
Delete From Quarantine	Deletes all files from Quarantine. This command only appears on the Risk log > Action drop-down list. See: How to delete Quarantined items from the Symantec Endpoint Protection Manager
Collect File Fingerprint List	Generates a non-editable file fingerprint list from the selected clients. The collected fingerprint list appears on the Policies tab under Policy Components > File Fingerprint Lists. Typically, you run this command on a single computer or small group of computers. If you select multiple computers, the command collects a separate list for each computer. • 14.3 RU5 and later creates a list with both the more secure SHA-256 and the MD5 file fingerprints. • 14.3 RU4 and earlier creates a list with the MD5 file fingerprints only. Note: Mac and Linux client computers do not process this command.

More information

[Symantec Endpoint Protection features based on platform](#)

Running commands on client computers from the console

You can manually run commands on the client computer at any time, such as starting or canceling a scan. On managed clients, the commands that you run from the management server override the commands that the user runs. The order in which commands are processed on the client computer differs from command to command. Regardless of where the command is initiated, the commands are processed in the same way. See:

[What are the commands that you can run on client computers?](#)

You run these commands from the following locations:

- The **Clients** page.
- The **Computer Status** log. You can run the **Cancel All scans** and **Start Power Eraser Analysis** commands from the **Computer Status** log only.
- The **Risk** Log. You can run the **Delete from Quarantine** command from the **Risk** log only. See:
[How to delete Quarantined items from the Symantec Endpoint Protection Manager](#)

If you start a scan, you can also cancel it immediately.

To run commands on the client computer from the Clients page

1. In the console, click **Clients**.
2. Do one of the following actions for groups or computers:

-
- In the left pane, right-click the group, and then click **Run a command on the group > command**
 - Click the **Clients** tab, right-click the computers, and then click **Run command on computers > command**
3. In the message that appears, click **Yes**.

To run a command from the Computer Status log

1. Click **Monitors > Logs > the Computer Status** log type, and then click **View Log**.
2. Select a command from the **Command** list box, select the computers, and then click **Start**.

NOTE

You can cancel an in-progress scheduled scan or a scan that you started by clicking **Cancel All Scans** from the command list.

To view the command results

1. Click **Monitors**.
2. On the **Command Status** tab, select a command in the list, and then click **Details**.

NOTE

You can also cancel a scan in progress by clicking the **Cancel Scan** icon in the **Command** column of the scan command.

Ensuring that a client does not restart

You can use the following procedure to ensure that any Symantec Endpoint Protection client computer does not restart. For example, you may want to set this value on the servers that run the Symantec Endpoint Protection client. Setting this registry key ensures that the server does not restart if an administrator issues a **Restart computer** command on its group from the console.

To ensure that a client does not restart

1. On the client computer, open the registry editor.
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC`.
3. Add the following line to the registry:

```
DisableRebootCommand REG_DWORD 1
```

Switching a Windows client between user mode and computer mode

You add Windows clients to be in either user mode or computer mode, based on how you want to apply policies to the clients in groups. After a user or a computer is added to a group, it assumes the policies that were assigned to the group.

When you add a client, it defaults to computer mode, which takes precedence over user mode. Symantec recommends that you use computer mode. Linux clients and Mac clients are only installed in computer mode.

Table 146: User mode vs. computer mode

Mode	Description
Computer mode	The client computer gets the policies from the group of which the computer is a member. The client protects the computer with the same policies, regardless of which user is logged on to the computer. The policy follows the group that the computer is in. Computer mode is the default setting. Many organizations configure a majority of clients in computer mode. Based on your network environment, you might want to configure a few clients with special requirements as users. You cannot switch from user mode to computer mode if the computer name is already in another group. Switching to computer mode deletes the user name of the client from the group and adds the computer name of the client into the group. Clients that you add in computer mode can be enabled as unmanaged detectors, and used to detect unauthorized devices. See: Configuring a client to detect unmanaged devices
User mode	The client computer gets the policies from the group of which the user is a member. The policies change, depending on which user is logged on to the client. The policy follows the user. If you import your existing group structure into Symantec Endpoint Protection Manager from Microsoft Active Directory or LDAP directory servers to organize clients by user, use user mode. You cannot switch from computer mode to user mode if the user's logon name and the computer name are already contained in any group. Switching to user mode deletes the computer name of the client from the group. It then adds the user name of the client into the group. See: Importing existing groups and computers from an Active Directory or an LDAP server

When you deploy a client installation package, you specify which group the client goes in. You can later specify the client to be in user mode or computer mode. If the client later gets deleted or disconnected and then gets added again and reconnected, the client returns to the original group. However, you can configure the client to stay with the group it was last moved to in user mode or computer mode. For example, a new user might log on to a client that is configured in user mode. The client then stays in the group that the previous user was in.

You configure these settings by clicking **Clients > Policies**, and then **Communications Settings**. See:

[Communications Settings for <group_name>](#)

To switch a Windows client between user mode and computer mode

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group that contains the user or computer.
3. On the **Clients** tab, right-click the computer or the user name in the table, and then select either **Switch to Computer Mode** or **Switch to User Mode**.

This mode is a toggle setting so one or the other always displays. The information in the table changes to reflect the new setting.

Configuring a client to detect unmanaged devices

Unauthorized devices can connect to the network in many ways, such as physical access in a conference room or rogue wireless access points. To enforce policies on every endpoint, you must be able to quickly detect the presence of new devices in your network. You must determine whether the devices are secure. You can enable any client as an unmanaged detector to detect the unknown devices. Unknown devices are unmanaged devices that do not run Symantec Endpoint Protection client software. If the unmanaged device is a computer, you can install the Symantec Endpoint Protection client software on it.

When a device starts up, its operating system sends the following traffic to the network to let other computers know of the device's presence:

-
- Address Resolution Protocol (ARP) traffic (ICMPv4)
 - Neighbor Discovery Protocol (NDP) traffic (ICMPv6).
- ICMPv6 is supported as of version 14.2.

A client that is enabled as an unmanaged detector collects and sends this packet information to the management server. The management server searches the packet for the device's MAC address and the IP address. The server compares these addresses to the list of existing MAC and IP addresses in the server's database. If the server cannot find an address match, the server records the device as new. You can then decide whether the device is secure. Because the client only transmits information, it does not use additional resources.

You can configure the unmanaged detector to ignore certain devices, such as printers. You can also set up email notifications to notify you when the unmanaged detector detects an unknown device.

To configure the client as an unmanaged detector, you must do the following actions:

- Enable Network Threat Protection. See:
[Running commands on client computers from the console](#)
- Switch the client to computer mode. See:
[Switching a Windows client between user mode and computer mode](#)
- Install the client on a computer that runs all the time.

As of 14.3 RU1, enabling the Linux client as an unmanaged detector is deprecated.

To configure an unmanaged detector

1. In the console, click **Clients**.
2. Under **Clients**, select the group that contains the client that you want to enable as an unmanaged detector.
3. On the **Clients** tab, right-click the client that you want to enable as an unmanaged detector, and then click **Enable as Unmanaged Detector**.
4. To specify one or more devices to exclude from detection by the unmanaged detector, click **Configure Unmanaged Detector**.
5. In the **Unmanaged Detector Exceptions for client name** dialog box, click **Add**.
6. In the **Add Unmanaged Detector Exception** dialog box, click one of the following options:
 - **Exclude detection of an IP address range**, and then enter the IP address range for several devices.
 - **Exclude detection of a MAC address**, and then enter the device's MAC address.
7. Click **OK** > **OK**.
8. To display the list of unauthorized devices that the client detects, in the console, click **Home**.
9. On the **Home** page, in the **Security Status** section, click **More Details**.
10. In the **Security Status Details** dialog box, scroll to the **Unknown Device Failures** table.
11. Close the dialog box.

To see if unmanaged clients are being detected

1. Go to the **Home** page and click **View Details** in the **Security Status** area.
2. When the **Security Status Details** window appears, click **Unknown Device Failures**.
Total Detected Unknown Devices shows how many devices are unmanaged. This includes access points, routers, switches and other devices in addition to computers.
3. To filter extraneous devices, go to the **Clients** page and right-click the unmanaged detector.
4. Click **Configure Unmanaged Detector** and add the IP or Mac addresses of the devices to be filtered.

Password-protecting the Symantec Endpoint Protection client

You can increase security against ransomware attacks by requiring password protection on the client computer whenever users perform certain tasks. Ransomware attacks can stop the client service and then launch an attack.

You should require the users to type a password when users try to do certain actions, such as stopping the client service (smc).

NOTE

As of 14.3 RU4, a message appears to remind you to enable at least one of these options.

For more information, see:

[Preventing and allowing users to change the client's user interface](#)

To password-protect the client

1. In the console, click **Clients**.
2. Under **Clients**, select the group for which you want to set up password protection.
3. On the **Policies** tab, under **Location-independent Policies and Settings**, click **Password**.

Earlier versions of Symantec Endpoint Protection may have some options that are worded differently, but you can still password-protect the client from the **Policies** tab.

4. In the **Client Password Settings** window, check any or all of the check boxes.

If the boxes are grayed out, this group inherits policies from a parent group. Before you can proceed, you must either edit the policy in the parent group or disable inheritance for this group. See:

[Disabling a group's inheritance](#)

5. In the **Password** and **Confirm password** text boxes, type the same password.

You can create a password that is between 6 to 256 characters in length.

If you see a message that the password strength is not acceptable, consider increasing the strength of your password. However, you may still be able to save the password.

Check **Apply password settings to non-inherited sub groups** to modify the password protection settings for any child group that does not inherit its settings from a parent. This setting appears for a parent group only.

6. Click **OK**.

Preventing users from disabling the Symantec Endpoint Protection client

As the Symantec Endpoint Protection Manager administrator, you prevent users from disabling protection on the client computer by locking the policy options or by setting the user control level. The method you use depends on the type of policy and when the policy was introduced in the Symantec Endpoint Protection Manager. For example, the firewall policy (version 11) uses a control level, whereas Virus and Spyware Protection policy (version 12.1.x) uses a lock.

NOTE

When you create a new policy, all the settings are unlocked by default. Client users can change the settings, which is a security issue. Therefore, Symantec recommends that you block users from disabling protection and changing the settings. You may want to allow client users to disable protection if you need to troubleshoot problems on the client computer or to allow small internal groups of developers to test internally developed applications.

Step 1: Lock policy settings using the padlock

You can lock and unlock some policy settings by clicking the padlock. Client users cannot change locked settings. A padlock icon appears next to a lockable setting. You can lock and unlock Virus and Spyware Protection settings, Tamper Protection settings, Submissions settings, and intrusion prevention settings.



☒ Enable Auto-Protect

To lock policies using the padlock

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the **Policies** tab.
3. Expand **Location-specific Policies**, and next to a policy, click **Tasks > Edit Policy > Edit Shared**.
4. In each policy, lock the padlock for the following settings.

Policy	Policy
Virus and Spyware Protection	Under Windows Settings, lock: • Auto-Protect > Enable Auto-Protect • Download Protection > Enable Download Insight to detect potential risks downloaded files based on file reputation • SONAR > Enable SONAR (14.3 RU4 and earlier) • SONAR > Enable Suspicious Detection Behavior (14.3 RU4 and earlier) • Early Launch Anti-Malware Driver > Enable Symantec early launch anti-malware • Internet Email Auto-Protect > Enable Internet Email Auto-Protect (14.2 and earlier) • Microsoft Outlook Auto-Protect > Enable Microsoft Outlook Auto-Protect • Lotus Notes Auto-Protect > Enable Lotus Notes Auto-Protect (14.2 and earlier) Under Global Scan Options, lock: • Enable Insight for • Enable Bloodhound heuristic virus detection
Intrusion Prevention	Under Intrusion Prevention, lock: Enable Network Intrusion Prevention Enable Browser Intrusion Prevention Enable URL reputation
Memory Exploit Mitigation	Memory Exploit Mitigation > Enable Memory Exploit Mitigation
Web and Cloud Access Protection	Under Web and Cloud Access Protection , lock Enable Web and Cloud Access Protection

Step 2: Lock policy settings using the user control levels

To lock the Firewall and the Application and Device Control policy, you change the user control level from client control to server control.

NOTE

If you do not want to change policies for all groups, disable policy inheritance on the group on which you want to make changes. If you edit a shared policy, the edited policy applies to every group to which the shared policy applies, even with policy inheritance disabled.

To lock the Firewall and Application and Device Control policies

1. In the console, click **Clients**.
2. Click the client group that you want to restrict, and then click the **Policies** tab.
3. Expand **Location-specific Settings**.
4. To the right of **Client User Interface Control Settings**, click **Tasks > Edit Settings**.
5. Click **Server control** or **Mixed control**, and then click **Customize**.
6. On the **Client User Interface Settings** dialog box (server control) or tab (mixed control), uncheck:
 - a. **Allow the following users to enable and disable the firewall**
 - b. **Allow user to enable and disable the application device control**
7. Click **OK > OK**.

For information on the user control levels, see: [Allowing users to change settings on the Symantec Endpoint Protection client user interface](#)

Step 3: Update the client policy

After you make these changes, the clients in the group receive the updated policies depending on the group's communication settings:

- If the group is in push mode, Symantec Endpoint Protection Manager prompts the client to check in with a few seconds.
- If the group is in pull mode, the client checks in on the next scheduled heartbeat.

NOTE

If you want them to have it sooner than the next heartbeat, you can prompt the client to check in and update its policy by updating the policy from the Symantec Endpoint Protection client. See:

[Updating client policies](#)

After the client updates the policy, **Disable Symantec Endpoint Protection** is grayed out when the client user right-clicks the Symantec Endpoint Protection notification area icon.

NOTE

If the **Disable Symantec Endpoint Protection** option is not grayed out, make sure that you locked all policy settings for the group.

Allowing users to change settings on the Symantec Endpoint Protection client user interface

What settings can users change on the client user interface?

On managed clients, you can make many protection settings available for the user can configure on the client. For example, you can allow the client user to add firewall rules or specify an action when a scan finds a detection.

You allow client users to change some settings using the following ways, depending on the policy type or setting:

- *Locking and unlocking a padlock* (SEPM version 12.1.x and later): All other policies except for the Firewall and the Application and Device Control policy. Any setting in the Symantec Endpoint Protection Manager that has a padlock next to it is a setting that you can allow or block the client user from changing.
- *User control levels*: Firewall policy and Application and Device Control policy and client user interface settings, such as displaying the client shield icon.

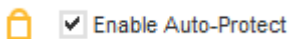
You use the user control levels to give the client user control of specific features.

For a list of the settings you enable or block on the client, see: [Client User Interface Mixed Control Settings: Client/Server Control Settings](#) and [Client User Interface Settings](#)

The user does not have access to all of the client features.

Locking client settings with a padlock

You can lock and unlock some policy settings by clicking the padlock. Client users cannot change locked settings. A padlock icon appears next to a lockable setting. You can lock and unlock most policy settings except for in the Firewall and Application and Device control. You configure those by using the user control levels.



About user control levels

You can configure user interface settings on the client if you do either of the following tasks:

- Set the client user control level to server control.
- Set the client user control level to mixed control and set the parent feature on the **Client/Server Control Settings** tab to **Server**.

For example, you can set the **Show/Hide notification area icon** option to **Client**. The notification area icon appears on the client and the user can choose to show or hide the icon. If you set the **Show/Hide notification area icon** option to **Server**, you can choose whether to display the notification area icon on the client.

NOTE

Most of these settings apply to the Windows client only. You can configure a few options on the Mac client in server control only.

The user control level also determines whether the client user interface can be invisible, display a partial set of features, or display in full.

If you set the client to **Mixed control** or **Server control** but do not lock the options, then the user can change the settings. These changes remain in place until the next heartbeat with Symantec Endpoint Protection Manager. Locking the policy options in the various policies ensures that the client user cannot make changes to the settings, even in **Client control**.

Some managed settings have dependencies. For example, users may have permission to configure firewall rules, but cannot access the client user interface. Because users do not have access to the **Configure Firewall Rules** dialog box, they cannot create rules.

NOTE

Windows users who are not the Administrators group cannot change settings in the Symantec Endpoint Protection client user interface, regardless of the **Location-specific Settings** configuration. Windows 10 Administrators can still disable the product through the notification area icon even after you set these options. However, they cannot disable the individual protection technologies through the client user interface.

Clients that run in **Client control** or **Mixed control** switch to **Server control** when the server applies a Quarantine policy.

More information

For more information on the differences between the three user control levels, see: [Client User Interface Control Settings for <group name>](#)

For a list of the settings you can enable, see: [Client User Interface Mixed Control Settings: Client/Server Control Settings](#) and [Client User Interface Settings](#)

Locking and unlocking settings using the user control levels

To lock and unlock settings

1. On the **Clients** page, and select the group that contains the clients you want to be affected.
2. On the **Policies** tab, expand **Location-specific Settings**.
3. To the right of **Client User Interface Control Settings**, click **Tasks** and then click **Edit Settings**.
4. Select **Server control** or **Mixed control** and then click **Customize**, if one of these options is not already set.
If you select **Client control**, click **OK**. The client user can configure any of the settings in the Client User Interface dialog box.
 - If you select **Server control**, the **Client User Interface Settings** dialog box opens.
On the **Client User Interface Settings** tab, check the option's check box so that the option is available on the client.
 - If you select **Mixed control** the **Client User Interface Mixed Control Settings** dialog box opens. Do one of the following actions:

-
- So that you can configure a setting from the management server only, lock an option by clicking **Server**. Any Virus and Spyware Protection settings that you set to **Server** override the settings on the client.
 - So that the client user can configure a setting on the client unlock an option by clicking **Client**. **Client** is selected by default for all settings except the Virus and Spyware settings.

For some of the options that you set to **Server**, click the **Client User Interface Settings** tab to configure them. For example, to enable firewall settings, configure them in the Firewall policy.

For information on where in the console you configure the remaining options that you set to **Server**, click **Help**.

[Enabling communications for network services instead of adding a rule](#)

[Enabling network intrusion prevention or browser intrusion prevention](#)

[Configuring firewall settings for mixed control](#)

5. Click **OK** > **OK**.

Collecting user information

You can prompt users on the client computers to type information about themselves during the client software installation process or during policy updates. You can collect information such as the employee's mobile phone number, job title, and email address. After you collect this information, you must maintain and update it manually.

This information is useful when the management server detects which client computers have a problem, such as infected or out-of-definitions. You can then find where the computer is and who uses it.

NOTE

After you enable the message to appear on the client computer for the first time, and the user responds with the requested information, the message does not appear again. Even if you edit any of the fields or disable and enable the message again, the client does not display a new message. However, the user can edit the information at any time, and the management server retrieves that information.

For more information, see:

[Managing client installation packages](#)

To collect user information

1. In the console, click **Admin**, and then click **Install Packages**.
2. In the **Install Packages** pane, click **Client Install Packages**.
3. Under **Tasks**, click **Set User Information Collection**.
4. In the **Set User Information Collection** dialog box, check **Collect User Information**.
5. In the **Pop-up Message** text box, type the message that you want users to read when they are prompted for information.
6. If you want the user to have the ability to postpone user information collection, check **Enable Remind Me Later**, and then set a time in minutes.
7. Under **Select the fields that will be displayed for the user to provide input**, choose the type of information to collect, and then click **Add**.

You can select one or more fields simultaneously by pressing the Shift key or the Control key.

8. In the Optional column, check the check box next to any fields that you want to define as optional for the user to complete.
9. Click **OK**.

Checking on your Mac client using AppleScript scripts

(For 14.3 RU2 and later)

AppleScript integration with Symantec Endpoint Protection client for Mac lets you create and run AppleScript scripts to query or control your Mac client.

Predefined scripts for querying the Mac client are not available. You will have the flexibility to create the scripts according to your requirements.

You can create and run the scripts in the Script Editor or you can run them from the command line. Using the Mac features, you can also schedule the scripts to run automatically at a specified time.

To create and run an AppleScript script in the Script Editor:

1. On your Mac device, open the Script Editor, and create a script that you want to run on your Mac device.
You can use the script examples given below.
2. To test the script, click **Run** on the toolbar.
3. Save the script in a format that best meets your needs.

To run an AppleScript script from the command line:

1. On your Mac device, open the Terminal window.
2. Run the script that you want.

Table 147: Examples of AppleScript scripts for Mac client

Action	Script Examples
Get last scan time	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" get last scan time end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" to get last scan time'
Get product version	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" get version end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" to get version'
Get content versions	Script to run in the Script Editor: tell application "Symantec Endpoint Protection" get definition information end tell Script to run from the command line: osascript -e 'tell app "Symantec Endpoint Protection" to get definition information'

Action	Script Examples
Run LiveUpdate	Script to run in the Script Editor: <pre>tell application "Symantec Endpoint Protection" activate tell main window to run LiveUpdate end tell</pre> Script to run from the command line: <pre>osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to run LiveUpdate' -e 'end tell'</pre>
Run QuickScan	Script to run in the Script Editor: <pre>tell application "Symantec Endpoint Protection" activate tell main window to quick scan end tell</pre> Script to run from the command line: <pre>osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to quick scan' -e 'end tell'</pre>
Run FullScan	Script to run in the Script Editor: <pre>tell application "Symantec Endpoint Protection" activate tell main window to full scan disks {"/"} end tell</pre> Script to run from the command line: <pre>osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to full scan disks' {"/"}' -e 'end tell'</pre>
Run FileScan	Script to run in the Script Editor: <pre>tell application "Symantec Endpoint Protection" activate tell main window to full scan files {"/tmp"} end tell</pre> Script to run from the command line: <pre>osascript -e 'tell app "Symantec Endpoint Protection" -e 'activate' -e 'tell main window to scan files' {"/tmp"}' -e 'end tell'</pre>

Managing your Linux client using the command line tool (sav)

The Linux client command line tool lets you control and check on your Linux client.

IMPORTANT

Root privilege is required to use this tool.

To manage your Linux Agent using the command line tool:

1. On a Linux client computer, navigate to the following location:
`/opt/Symantec/sdcssagent/AMD/tools`
2. Run the sav command as follows:
`./sav [options] command`

Table 148: Options for sav

Option	Description	Applies to
-h --help	Displays available options and commands for sav.	As of 14.3 RU2
-q --quiet	Quiet	As of 14.3 RU2

Table 149: Commands for sav

Option	Description	Applies to
autoprotect -d --disable	Disables Auto-Protect.	As of 14.3 RU2
autoprotect -e --enable	Enables Auto-Protect. To check the Auto-Protect status, run the following command: [root@localhost tools]# cat /proc/sisap/status grep -i MODE The reply can be one of the following commands: - mode=ENA (if enabled) - mode=DIS (if disabled)	As of 14.3 RU2
info -a --autoprotect	Displays the status of auto-protect on the computer.	As of 14.3 RU4
info -d --defs	Shows the version and date of the current virus and security risk definitions used on the device.	As of 14.3 RU3
info -e --engine	Shows the version of the scan engine that the device is using.	As of 14.3 RU3
info -p --product	Shows the Symantec Agent version in use on the device.	As of 14.3 RU3
liveupdate -u --update	Runs LiveUpdate immediately.	As of 14.3 RU3
manage -i --import <file>	Imports the <i>sylink.xml</i> file from the specified location.	As of 14.3 RU2
manualscan -s --scan <file list>	Starts a manual scan. <file list> specifies the file and directory list to scan. To specify this list, type a list of files and directories that are separated by line feeds and ending with an end of file signal, such as CTRL-D. If a directory is specified, all subdirectories are also scanned. Wildcard characters are supported. If you specify a hyphen (-) instead of a list of files and directories, then the list of path names is read from the standard input. You can use commands that produce a list of files or path names that are separated by line feeds. Submitting a long list of items to this command can negatively affect performance. Symantec recommends that you limit lists to a maximum of a few thousand items.	As of 14.3 RU3
manualscan -t --stop	Stops a manual scan that is in progress.	As of 14.3 RU3
quarantine -d --delete <ID>	Delete the specified item from the Quarantine. To view the ID of an item, list the items that are in the Quarantine.	As of 14.3 RU4
quarantine -i --info <ID>	Provides detailed information about the quarantined item. To view the ID of an item, list the items that are in the Quarantine.	As of 14.3 RU4
quarantine -l --list	List all of the items that are in the local Quarantine.	As of 14.3 RU4
quarantine -r --restore <ID>	Restores the quarantined item that is specified. To view the ID of an item, list the items that are in the Quarantine.	As of 14.3 RU4

Option	Description	Applies to
<pre>scheduledscan -c --create scan_id parameters pathname</pre>	Creates a new local scheduled scan that is identified by <code>scan_id</code>, which must be unique. If an existing <code>scan_id</code> is specified, the existing <code>scan_id</code> scheduled scan is updated. The <code>pathname</code> specifies the file and directory list to scan. To specify this list, type a list of files and directories separated by spaces. If a directory is specified, all subdirectories are also scanned. Wildcard characters are supported. • <code>-f --frequency [daily weekly monthly]</code> Required. Specifies the scan frequency. • <code>-i --interval [HH:MM DDD D]</code> Specifies the interval between scans. Depends on the frequency. If frequency is daily, the interval must be HH:MM, where HH = the hour (00 - 23) and MM = the minute (00-59). If frequency is weekly, the interval must be DDD, where DDD = one of Sun, Mon, Tue, Wed, Thu, Fri, Sat. If frequency is monthly, the interval must be D, where D = any value from 1 to 31. • <code>-t --time [HH:MM]</code> HH = the hour (00 - 23) and MM = the minute (00 - 59). Not used for daily frequency. Submitting a long list of items to this command can negatively affect performance. Symantec recommends that you limit lists to a maximum of a few thousand items.	As of 14.3 RU4
<pre>scheduledscan -d --delete scan_id</pre>	Deletes the local scheduled scan that is specified by <code>scan_id</code>. Administrator-defined scheduled scans cannot be deleted manually.	

More information

[Troubleshooting the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux](#)

Managing remote clients

Your network may include some clients that connect to the network from different locations. You may need to manage these clients differently from the clients that connect only from within the network. You may need to manage some clients that always connect remotely over a VPN, or clients that connect from multiple locations because employees travel. You may also need to manage security for some computers that are outside your administrative control. For example, you may allow customers, contractors, vendors, or business partners to have limited access to your network. Some employees may connect to your network using their own personal computers, and you may need to manage these clients differently.

In all these cases, you must deal with greater security risk. Connections may be less secure, or the client computers may be less secure, and you may have less control over some clients. To minimize these risks to your overall network security, you should assess the different kinds of remote access that clients have to your network. You can then apply more stringent security policies based on your assessment.

To manage the clients that connect to your network differently because of the security risks that they pose, you can work with Symantec Endpoint Protection's location awareness.

You apply different policies to clients that pose a greater risk to your network based on their location. A location in Symantec Endpoint Protection is defined as the type of connection that a client computer uses to connect to your network. A location can also include information about whether the connection is located inside or outside your corporate network.

You define locations for a group of clients. You then assign different policies to each location. Some security settings can be assigned to the entire group regardless of location. Some settings are different depending on location.

Table 150: Managing remote clients

Task	Description
Set up groups based on assessment of security risk	For more information, see: Managing groups of clients
Set up locations for groups of remote clients	For more information, see: Managing locations for remote clients
Configure communication settings for locations	For more information, see: Configuring communication settings for a location
Strengthen your security policies	For more information, see: About strengthening your security policies for remote clients
Turn on client notifications	For more information, see: About turning on notifications for remote clients
Customize client log management settings	Customize the log settings for remote clients, especially if clients are offline for several days. To reduce bandwidth and the load on your management servers, make the following changes: • Set clients to not upload their logs to the management server. • Set clients to upload only the client security logs. • Set filter log events to upload only specified events. Suggested events to upload include definition updates, or side effect repair failures. • Make the log retention time longer. Longer retention times let you review more virus and spyware event data.
Monitor remote clients	For more information, see: • About monitoring remote clients from the management server • Monitoring roaming Symantec Endpoint Protection clients from the cloud console

Managing locations for remote clients

You add locations after you set up the groups that you need to manage. Each group can have different locations if your security strategy requires it. In the Symantec Endpoint Protection Manager console, you set up the conditions that trigger automatic policy switching based on location. Location awareness automatically applies the security policy that you specify to a client, based on the location conditions that the client meets.

Location conditions can be based on a number of different criteria. These criteria include IP addresses, type of network connection, whether the client computer can connect to the management server, and more. You can allow or block client connections based on the criteria that you specify.

A location applies to the group you created it for and to any subgroups that inherit from the group. A best practice is to create the locations that any client can use at the My Company group level. Then, create locations for a particular group at the subgroup level.

It is simpler to manage your security policies and settings if you create fewer groups and locations. The complexity of your network and its security requirements, however, may require more groups and locations. The number of different security settings, log-related settings, communications settings, and policies that you need determines how many groups and locations you create.

Some of the configuration options that you may want to customize for your remote clients are location-independent. These options are either inherited from the parent group or set independently. If you create a single group to contain all remote clients, then the location-independent settings are the same for the clients in the group.

The following settings are location-independent:

- Custom intrusion prevention signatures
- System Lockdown settings
- Network application monitoring settings
- LiveUpdate content policy settings
- Client log settings
- Client-server communications settings
- General security-related settings, including location awareness and Tamper Protection

To customize any of these location-independent settings, such as how client logs are handled, you need to create separate groups.

Some settings are specific to locations.

As a best practice, you should not allow users to turn off the following protections:

- Auto-Protect
- Behavioral analysis
- Tamper Protection
- The firewall rules that you have created

Table 151: Location awareness tasks that you can perform

Tasks	Description
Plan locations	You should consider the different types of security policies that you need in your environment to determine the locations that you should use. You can then determine the criteria to use to define each location. It is a best practice to plan groups and locations at the same time. See: Managing groups of clients You may find the following examples helpful: • Setting up Scenario One location awareness conditions • Setting up Scenario Two location awareness conditions
Enable location awareness	To control the policies that are assigned to clients contingent on the location from which the clients connect, you can enable location awareness. See: Enabling location awareness for a client
Add locations	You can add locations to groups. See: Adding a location to a group
Assign default locations	All groups must have a default location. When you install the console, there is only one location, called Default. When you create a new group, its default location is always Default. You can change the default location later after you add other locations. The default location is used if one of the following cases occurs: • One of the multiple locations meets location criteria and the last location does not meet location criteria. • You use location awareness and no locations meet the criteria. • The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy. For more information, see: Changing a default location
Configure communications settings for locations	You can also configure the communication settings between a management server and the client on a location basis. See: Configuring communication settings for a location

More information

- [Managing remote clients](#)
- [Best Practices for Symantec Endpoint Protection Location Awareness](#)

Enabling location awareness for a client

To make the policies that are assigned to clients contingent on the client's connection location, you can enable location awareness for the client.

If you check **Remember the last location**, then when a client connects to the network, it is assigned the policy from the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the client can manually switch between any of the locations even when it is under server control. If a quarantine location is enabled, the client may switch to the quarantine policy after a few seconds.

If you uncheck **Remember the last location**, then when a client connects to the network, it is assigned the policy from the default location. The client cannot connect to the last-used location. If location awareness is enabled, then the client automatically switches to the appropriate policy after a few seconds. The policy that is associated with a specific location determines a client's network connection. If location awareness is disabled, the user can manually switch between any of the locations even when the client is under server control. If a quarantine location is enabled, the client may switch to the Quarantine Policy after a few seconds.

To enable location awareness for a client

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, select the group for which you want to implement automatic switching of locations.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
4. Under **Location-independent Policies and Settings**, click **General Settings**.
5. In the **General Settings** dialog box, on the **General Settings** tab, under **Location Settings**, check **Remember the last location**.

By default, this option is enabled. The client is initially assigned to the policy that is associated with the location from which the client last connected to the network.

6. Check **Enable Location Awareness**.

By default, location awareness is enabled. The client is automatically assigned to the policy that is associated with the location from which the user tries to connect to the network.

7. Click **OK**.

More information

[Adding a location to a group](#)

Adding a location to a group

When you add a location to a group, you specify the conditions that trigger the clients in the group to switch to the location. Location awareness is effective only if you also apply appropriate policies and settings to each location.

To add a location to a group

1. In the console, click **Clients**.
2. In the **Clients** page, under **Clients**, select the group for which you want to add one or more locations.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.

You can add locations only to groups that do not inherit policies from a parent group.

You can also click **Add Location** to run the **Add Location** wizard.

-
4. In the **Client** page, under **Tasks**, click **Manage Locations**.
 5. In the **Manage Locations** dialog box, under **Locations**, click **Add**.
 6. In the **Add Location** dialog box, type the name and description of the new location, and then click **OK**.
 7. To the right of the **Switch to this location when** box, click **Add**.
 8. In the **Type** list, select a condition, and then select the appropriate definition for the condition.
A client computer switches to the location if the computer meets the specified criteria.
 9. Click **OK**.
 10. To add more conditions, click **Add**, and then select either **Criteria with AND relationship** or **Criteria with OR relationship**.
 11. Click **OK**.

More information

[About strengthening your security policies for remote clients](#)

Changing a default location

When the Symantec Endpoint Protection Manager is initially installed, only one location, called Default, exists. At that time, every group's default location is Default. Every group must have a default location. When you create a new group, the Symantec Endpoint Protection Manager console automatically makes its default location Default.

You can specify another location to be the default location for a group after you add other locations. You may prefer to designate a location like Home or Road as the default location.

A group's default location is used if one of the following cases occurs:

- One of the multiple locations meets location criteria and the last location does not meet location criteria.
- You use location awareness and no locations meet the criteria.
- The location is renamed or changed in the policy. The client reverts to the default location when it receives the new policy.

To change a default location

1. In the console, click **Clients**.
2. On the **Clients** page, under **Clients**, click the group to which you want to assign a different default location.
3. On the **Policies** tab, uncheck **Inherit policies and settings from parent group "group name"**.
4. Under **Tasks**, click **Manage Locations**.
5. In the **Manage Locations** dialog box, under **Locations**, select the location that you want to be the default location.
6. Under **Description**, check **Set this location as the default location in case of conflict**.
The Default location is always the default location until you assign another one to the group.
7. Click **OK**.

More information

[Managing locations for remote clients](#)

Setting up Scenario One location awareness conditions

If you have remote clients, in the simplest case, it is a common practice to use the My Company group and three locations. This is Scenario One.

To manage the security of the clients in this scenario, you can create the following locations under the My Company group to use:

- Office clients that log on in the office.
- The remote clients that log on to the corporate network remotely over a VPN.
- The remote clients that log on to the Internet remotely, but not over a VPN.

Because the remote location with no VPN connection is the least secure, it has the most secure policies. It is a best practice to always make this location the default location.

NOTE

If you turn off My Company group inheritance and then you add groups, the added groups do not inherit the locations that you set up for the My Company group.

The following suggestions represent the best practices for Scenario One.

To set up the office location for the clients located in the office

1. On the **Clients** page, select the group for which you want to add a location.
2. On the **Policies** tab, under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.
4. Type a name for the location and optionally, add a description of it, and then click **Next**.
5. In the list box, click **Client can connect to management server** from the list, and then click **Next**.
6. Click **Finish**, and then click **OK**.
7. Under **Tasks**, click **Manage Locations**, and then select the location you created.
8. Click **Add**, and then click **Criteria with AND relationship**.
9. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
10. Click **If the client computer does not use the network connection type specified below**.
11. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
12. Click **OK** to exit the **Manage Locations** dialog box.

To set up the remote location for the clients logging in over a VPN

1. On the **Clients** page, select the group for which you want to add a location.
2. On the **Policies** tab, under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.
4. Type a name for the location and optionally, add a description of it, and then click **Next**.
5. In the list box, click **Network connection type**.
6. In the **Connection Type** list box, select the name of the VPN client that your organization uses, and then click **Next**.
7. Click **Finish**.
8. Click **OK**.

To set up the remote location for the clients not logging on over a VPN

1. On the **Clients** page, select the group for which you want to add a location.
2. On the **Policies** tab, under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.
4. Type a name for the location, optionally add a description of it, and then click **Next**.
5. In the list box, leave **No specific condition**, and then click **Next**.

By using these settings, this location's policies, which should be the strictest and most secure, are used as the default location policies.

6. Click **Finish**, and then click **OK**.

More information

- [Setting up Scenario Two location awareness conditions](#)
- [Managing remote clients](#)

Setting up Scenario Two location awareness conditions

In Scenario Two, you use the same two remote locations as specified in Scenario One and two office locations, for a total of four locations.

You would add the following office location:

- Clients in the office that log on over an Ethernet connection.
- Clients in the office that log on over a wireless connection.

It simplifies management to leave all clients under the default server control mode. If you want granular control over what your users can and cannot do, an experienced administrator can use mixed control. A mixed control setting gives the end user some control over security settings, but you can override their changes, if necessary. Client control allows users a wider latitude in what they can do and so constitutes a greater risk to network security.

Symantec suggests that you use client control only in the following situations:

- If your users are knowledgeable about computer security.
- If you have a compelling reason to use it.

NOTE

You may have some clients that use Ethernet connections in the office while other clients in the office use wireless connections. For this reason, you set the last condition in the procedure for wireless clients in the office. This condition lets you create an Ethernet location Firewall policy rule to block all wireless traffic when both kinds of connections are used simultaneously.

To set up the office location for the clients that are logged on over Ethernet

1. On the **Clients** page, select the group for which you want to add a location.
2. Under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.
4. Type a name for the location, optionally add a description of it, and then click **Next**.
5. In the list box, select **Client can connect to management server**, and then click **Next**.
6. Click **Finish**.
7. Click **OK**.
8. Under **Tasks**, click **Manage Locations**, and then select the location you created.
9. Beside **Switch to this location when**, click **Add**, and then select **Criteria with AND relationship**.
10. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
11. Click **If the client computer does not use the network connection type specified below**.
12. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
13. Click **Add** and then click **Criteria with AND relationship**.
14. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
15. Click **If the client computer uses the network connection type specified below**.
16. In the bottom list box, select **Ethernet**, and then click **OK**.
17. Click **OK** to exit the Manage Locations dialog box.

To set up the office location for the clients that are logged on over a wireless connection

1. On the **Clients** page, select the group for which you want to add a location.
2. Under **Tasks**, click **Add Location**.
3. In the **Add Location Wizard**, click **Next**.

-
4. Type a name for the location, optionally add a description of it, and then click **Next**.
 5. In the list box, click **Client can connect to management server**, and then click **Next**.
 6. Click **Finish**.
 7. Click **OK**.
 8. Under Tasks, click **Manage Locations**, and then select the location that you created.
 9. Beside Switch to this location when, click **Add**, and then click **Criteria with AND relationship**.
 10. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
 11. Click **If the client computer does not use the network connection type specified below**.
 12. In the bottom list box, select the name of the VPN client that your organization uses, and then click **OK**.
 13. Click **Add**, and then click **Criteria with AND relationship**.
 14. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
 15. Click **If the client computer does not use the network connection type specified below**.
 16. In the bottom list box, click **Ethernet**, and then click **OK**.
 17. Click **Add**, and then click **Criteria with AND relationship**.
 18. In the **Specify Location Criteria** dialog box, from the **Type** list, click **Network Connection Type**.
 19. Click **If the client computer uses the network connection type specified below**.
 20. In the bottom list box, click **Wireless**, and then click **OK**.
 21. Click **OK** to exit the **Manage Locations** dialog box.

More information

- [Setting up Scenario One location awareness conditions](#)
- [Managing remote clients](#)

Configuring communication settings for a location

By default, you configure communication settings between the management server and the client at the level of the group. However, you can also configure these settings for individual locations in a group. For example, you can use a separate management server for a location where the client computers connect through the VPN. To minimize the number of clients that connect to the management server at the same time, you can specify a different heartbeat for each location.

You can configure the following communication settings for locations:

- The control mode in which the clients run.
- The management server list that the clients use.
- The download mode in which the clients run.
- Whether to collect a list of all the applications that are executed on clients and send the list to the management server.
- The heartbeat interval that clients use for downloads.
- Whether the management server randomizes content downloads from the default management server or a Group Update Provider.

NOTE

Only some of these settings can be configured for Mac clients.

To configure communication settings for a location

-
1. In the console, click **Clients**.
 2. On the **Clients** page, select a group.
 3. On the **Policies** tab, under **Location-specific Policies and Settings**, under a location, expand **Location-specific Settings**.
 4. To the right of **Communications Settings**, click **Tasks**, and then uncheck **Use Group Communications Settings**.
 5. Click **Tasks** again, and then click **Edit Settings**.
 6. In the **Communications Settings for location name** dialog box, modify the settings for the specified location only.
 7. Click **OK**.

More information

- [Updating policies and content on the client using push mode or pull mode](#)
- [Managing locations for remote clients](#)
- [Managing groups of clients](#)

About strengthening your security policies for remote clients

When you manage remote users, you essentially take one of the following positions:

- Leave the default policies in place, so that you do not impede remote users in the use of their computers.
- Strengthen your default security policies to provide more protection for your network, even if it restricts what remote users can do.

In most situations, the best practice is to strengthen your security policies for remote clients.

Policies may be created as shared or unshared and assigned either to groups or to locations. A shared policy is one that applies to any group and location and can be inherited. A non-shared policy is one that only applies to a specific location in a group. Typically, it is considered a best practice to create shared policies because it makes it easier to change policies in multiple groups and locations. However, when you need unique location-specific policies, you need to create them as non-shared policies or convert them to non-shared policies.

More information

[Managing remote clients](#)

Best practices for Firewall policy settings for remote clients

The following table describes scenarios and best-practice recommendations.

Table 152: Firewall policy best practices

Scenario	Recommendation
Remote location where users log on without a VPN	- Assign the strictest security policies to clients that log on remotely without using a VPN. - Enable NetBIOS protection. Note: Do not enable NetBIOS protection for the location where a remote client is logged on to the corporate network through a VPN. This rule is appropriate only when remote clients are connected to the Internet, not to the corporate network. - Block all local TCP traffic on the NetBIOS ports 135, 139, and 445 to increase security.
Remote location where users log on through a VPN	- Leave as-is all the rules that block traffic on all adapters. Do not change those rules. - Leave as-is the rule that allows VPN traffic on all adapters. Do not change that rule. - Change the Adapter column from All Adapters to the name of the VPN adapter that you use for all rules that use the action Allow. - Enable the rule that blocks all other traffic. Note: You need to make all of these changes if you want to avoid the possibility of split tunneling through the VPN.
Office locations where users log on through Ethernet or wireless connections	Use your default Firewall policy. For the wireless connection, ensure that the rule to allow wireless EAPOL is enabled. 802.1x uses the Extensible Authentication Protocol over LAN (EAPOL) for connection authentication.

More information

- [Creating a firewall policy](#)
- [Enabling communications for network services instead of adding a rule](#)

About turning on notifications for remote clients

For your remote clients that are not logged on over VPN, it is a best practice to turn on client notifications for the following situations:

- Intrusion detections
You can turn on these notifications by using the location-specific server or, you can select the **Mixed control** option in the **Client User Interface Control Settings**. You can customize the settings on the **Client User Interface Settings** tab.
- Virus and security risks
You can turn on these notifications in the Virus and Spyware Protection policy.

Turning on notifications helps to ensure that remote users are aware when a security problem occurs.

More information

[Managing remote clients](#)

About monitoring remote clients from the management server

Notifications and logs are essential to maintain a secure environment. In general, you should monitor your remote clients in the same way that you monitor your other clients. You should always check to see that your protections are up to date and that your network is not currently under attack. If your network is under attack, then you want to find out who is behind the attack and how they attacked.

Your Home page preference settings determine the time period for which Symantec Endpoint Protection Manager displays data. By default, the data on the Home page represents only the clients that connected in the past 12 hours. If you have

many clients that are frequently offline, your best monitoring option is to go to the logs and reports. In the logs and reports, you can filter the data to include offline clients.

Even if you restrict some of the client log data that mobile clients upload, you can check the following displays.

Table 153: Displays to monitor remote client security

Display	Description
Home > Endpoint Status	Displays whether the content is up to date or to see if any of the protections are turned off. You can check the following status conditions: • Content dates and version numbers • Client connections • Enabled and disabled protections You can click Details to see the status for each client.
Home > Security Status	Displays the system security overview. View the Virus and Risks Activity Summary to see if your network is under attack. You can click Details to see the status for each security protection technology.
Home > Virus and Risks Activity Summary	Displays the detected virus and risk activity, and the actions taken, such as cleaned, blocked, or quarantined.
Monitors > Summary Type > Network Threat Protection	Displays the information about attack types and sources.

More information

- [Managing remote clients](#)
- [Monitoring roaming Symantec Endpoint Protection clients from the cloud console](#)

Managing administrator accounts and passwords

You can use administrator accounts to manage Symantec Endpoint Protection Manager datacenters. Administrators log on to Symantec Endpoint Protection Manager to change policy settings, manage groups, run reports, and install client software, as well as other management tasks.

The default account is a system administrator account, which provides access to all features. You can also add a more limited administrator account, for administrators who need to perform a subset of tasks.

For a small company, you may only need one administrator and one domain. For a large company with multiple sites and Windows domains, you most likely need multiple administrators, some of whom have more access rights than others. You may also need to add multiple domains within Symantec Endpoint Protection Manager.

You manage domains and administrator accounts and their passwords on the **Admin** page.

Table 154: Account administration

Task	Description
Decide whether to add multiple domains	Decide whether to add domains. See: About domains Adding a domain Switching to the current domain
Add administrator accounts	Add accounts for administrators who need access to the Symantec Endpoint Protection Manager console. - Add the types of administrator accounts that you need, and the level of access rights. See: About administrator accounts and access rights Adding an administrator account and setting access rights - Choose a method to authenticate administrator for when they log on to Symantec Endpoint Protection Manager (optional). By default, the Symantec Endpoint Protection Manager database authenticates the administrator's credentials. See: Choosing the authentication method for administrator accounts
Unlock or lock an administrator account	By default, Symantec Endpoint Protection Manager locks out an administrator after a user tries to log on to Symantec Endpoint Protection Manager using the administrator account too many times. You can configure these settings to increase the number of tries or time the administrator is locked out. If an administrator is locked out of their account, they must wait the specified time before logging on again. You cannot unlock an account during the lockout interval. See: Unlocking an administrator's account after too many logon attempts
Change and reset lost passwords	- Change the password for your account or another administrator's account. See: Changing the password for an administrator account or the default database - Reset a lost password using the Forgot your password? link that appears on the management server logon screen. The administrator receives an email that contains a link to activate a temporary password. See: Resetting a forgotten Symantec Endpoint Protection Manager password Displaying the Forgot your password? link so that administrators can reset lost passwords - Allow administrators to save their user name and password on the management server logon screen. See: Displaying the Remember my user name and check boxes on the logon screen - Force the administrator's logon password to expire after a certain number of days. See: Displaying the Remember my user name and check boxes on the logon screen
Configure logon options for Symantec Endpoint Protection Manager	You can configure the following logon options for each type of administrator: - Display a message for administrators to read before they log on. See: Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console - Allow or block log on access to the management console, so that certain administrators can, or cannot, log on remotely. See: Granting or blocking access to remote Symantec Endpoint Protection Manager consoles - Changing how long an administrator can stay logged on to the management server. See: Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console For more information, see: Logging on to the Symantec Endpoint Protection Manager console

About administrator accounts and access rights

When you install the Symantec Endpoint Protection Manager, a default system administrator account is created, called `admin`. The system administrator account gives an administrator access to all the features in Symantec Endpoint Protection Manager.

To help you manage security, you can add additional system administrator accounts, domain administrator accounts, and limited administrator accounts. Domain administrators and limited administrators have access to a subset of Symantec Endpoint Protection Manager features.

You choose which accounts you need based on the types of roles and access rights you need in your company. For example, a large company may use the following types of roles:

- An administrator who installs the management server and the client installation packages. After the product is installed, an administrator in charge of operations takes over. These administrators are most likely system administrators.
- An operations administrator maintains the servers, databases, and installs patches. If you have a single domain, the operations administrator could be a domain administrator who is fully authorized to manage sites.
- An antivirus administrator, who creates and maintains the Virus and Spyware Protection policies and LiveUpdate policies on the clients. This administrator is most likely to be a limited administrator.
- A desktop administrator, who is in charge of security and creates and maintains the Firewall policies and Intrusion Prevention policies for the clients. This administrator is most likely to be a domain administrator.
- A help desk administrator, who creates reports and has read-only access to the policies. The antivirus administrator and desktop administrator read the reports that the help desk administrator sends. The help desk administrator is most likely to be a limited administrator who is granted reporting rights and policy rights.

Table 155: Administrator roles and responsibilities

Administrator role	Responsibilities
System administrator	System administrators can log on to the Symantec Endpoint Protection Manager console with complete, unrestricted access to all features and tasks. A system administrator can create and manage other system administrator accounts, domain administrator accounts, and limited administrator accounts. A system administrator can perform the following tasks: • Manage all domains. • Administer licenses. • View and manage all console settings. • Manage the databases and management servers.
Administrator	Administrators are domain administrators who can view and manage a single domain. A domain administrator has the same privileges as a system administrator, but for a single domain only. By default, the domain administrator has full system administrator rights to manage a domain, but not a site. You must explicitly grant site rights within a single domain. Domain administrators can modify the site rights of other administrators and limited administrators, though they cannot modify the site rights for themselves. A domain administrator can perform the following tasks: • Create and manage administrator accounts and limited administrator accounts within a single domain. Domain administrators cannot modify their own site rights. System administrators must perform this function. • Run reports, manage sites, and reset passwords. • Cannot administer licenses. Only system administrators can administer licenses. For more information, see: About domains
Limited administrator	Limited administrators can log on to the Symantec Endpoint Protection Manager console with restricted access. Limited administrators do not have access rights by default. A system administrator role must explicitly grant access rights to allow a limited administrator to perform tasks. Parts of the management server user interface are not available to limited administrators when you restrict access rights. For example: • Limited administrators without reporting rights cannot view the Home, Monitors, or Reports pages. • Limited administrators without policy rights cannot view or modify the policy. In addition, they cannot apply, replace, or withdraw a policy.

More information

- [Adding an administrator account and setting access rights](#)
- [Managing administrator accounts](#)

Adding an administrator account and setting access rights

As a system administrator, you can add another system administrator, administrator, or limited administrator. As an administrator within a domain, you can add other administrators with access rights equal to or less restrictive than your own. Administrators can add limited administrators and configure their access rights.

To add an administrator account

1. In the console, click **Admin > Administrators**.
2. Under **Tasks**, click **Add an administrator**.
3. In the **Add Administrator** dialog box, on the **General** tab, enter the user name and email address.
4. On the **Access Rights** tab, specify the type of administrator account.

If you add an account for a limited administrator, you must also specify the administrator's access rights. Limited administrator accounts that are not granted any access rights are created in a disabled state and the limited administrator cannot log on to the management server. See:

[About administrator accounts and access rights](#)

5. On the **Authentication** tab, under **Symantec Endpoint Protection Manager Authentication**, type the password the administrator should use to log on.

When the administrator logs on to the Symantec Endpoint Protection Manager, Symantec Endpoint Protection Manager verifies with the database that the user name and password are correct. See:

[Choosing the authentication method for administrator accounts](#)

6. Click **OK**.

Choosing the authentication method for administrator accounts

You can choose from several authentication methods that the management server uses to check administrators' credentials before they log on.

For the third-party authentication methods, Symantec Endpoint Protection Manager has an entry in the database for the administrator account, but the third-party server validates the user name and password.

Table 156: Authentication methods

Type	When to use
Symantec Endpoint Protection Manager authentication (default)	Authenticates the administrators with the administrator's user name and password that are stored in the Symantec Endpoint Protection Manager database. When the administrator logs on to the management server, the management server verifies with the database that the user name and password are correct. You can display the Password never expires option so that an administrator's account does not expire. See: Enabling Symantec Endpoint Protection Manager logon passwords to never expire
Two-factor authentication	Authenticates the administrators with Symantec VIP authentication on their smartphone. Administrators provide a unique, one-time verification code when they log on, in addition to a password. For this option to be available, you must first add the appropriate PKCS keystore file and keystore's password. See: Configuring two-factor authentication with Symantec VIP

Type	When to use
RSA SecurID authentication	Authenticates the administrators by using RSA SecurID token (not software RSA tokens), RSA SecurID card, or RSA keypad card (not RSA smart cards). To authenticate administrators who use an RSA SecurID mechanism, first install the RSA Authentication Manager server and enable encrypted authentication for RSA SecurID. See: Using RSA SecurID authentication with Symantec Endpoint Protection Manager
Directory server authentication	Authenticates the administrators with an LDAP server or the Microsoft Active Directory server. To authenticate administrators using an Active Directory or LDAP directory server, you need to set up an account on the directory server. You must also establish a connection between the directory server and Symantec Endpoint Protection Manager. If you do not establish a connection, you cannot import users from an Active Directory server or synchronize with it. Note: Synchronization is only possible for Active Directory Servers. Synchronization with LDAP servers is not supported. For more information, see: • Connecting Symantec Endpoint Protection Manager to a directory server • Checking the authentication to a directory server
Smart card authentication	Authenticates the administrators who work as civilians or military personnel in U.S. Federal Agencies and who must use a PIV card or CAC to log on. See: Configuring Symantec Endpoint Protection Manager to authenticate administrators who log on with smart cards

To choose an authentication method for administrator accounts

1. Add an administrator account. See:
[Adding an administrator account and setting access rights](#)
2. On the **Authentication** tab, select the authentication method if you do not want to use **Symantec Endpoint Protection Manager Authentication** (default).
3. Click **OK**.
4. In the **Confirm Change** dialog box, type the password that you use to log on to Symantec Endpoint Protection Manager, and then click **OK**.

When you switch between authentication methods, you must type the administrator account's password.

Using RSA SecurID authentication with Symantec Endpoint Protection Manager

NOTE

In an IPv6 environment, you must install and enable the IPv4 stack on the Symantec Endpoint Protection Manager server to use RSA SecurID authentication.

(IPv6 networking is supported as of version 14.2.)

Configuring RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators

If you want to authenticate administrators who use the Symantec Endpoint Protection Manager with RSA SecurID, you must first enable encrypted authentication by configuring a connection to an RSA Authentication Manager server.

To configure RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators

1. Install an RSA Authentication Manager server, if necessary. Use RSA Authentication Manager 8.1.
2. Install and properly configure the RSA Authentication Agent on the Symantec Endpoint Protection Manager server to connect to the RSA server. Use RSA Authentication Agent 7.x.

-
3. Ensure that the Symantec Endpoint Protection Manager server registers as a valid host on the RSA Authentication Manager server.
 4. Ensure that the `sdconf.rec` file on the RSA Authentication Manager server is accessible on the network.
 5. Assign a synchronized SecurID card or key fob to a management server account; activate the logon name on the RSA Authentication Manager server.
 6. Ensure that the administrator has the RSA PIN or password available.
Symantec supports the following types of RSA logons:
 - RSA SecurID token (not software RSA tokens)
 - RSA SecurID card
 - RSA keypad card (not RSA smart cards)To log on to the management server with the RSA SecurID, an administrator needs a logon name, the token (hardware), and a PIN.

Installing the RSA Authentication Agent and configure the Symantec Endpoint Protection Manager server to use RSA SecurID authentication

To use RSA SecurID with Symantec Endpoint Protection Manager, you must install the RSA Authentication Agent on the Symantec Endpoint Protection Manager server and configure it as a SecurID Authentication client.

To install the RSA Authentication Agent

1. Install the software for the RSA Authentication Agent on the Symantec Endpoint Protection Manager server. You can install the software by running the Windows .msi file from the RSA Authentication Agent installation file.
2. Copy the `sdconf.rec` file from the RSA Authentication server to the Symantec Endpoint Protection Manager server. For earlier versions of RSA Authentication Agent, copy `nodesecret.rec`, `sdconf.rec`, and `agent_nsload.exe`.

To configure the Symantec Endpoint Protection Manager server to use RSA SecurID authentication

1. Log on to the Symantec Endpoint Protection Manager console, and then click **Admin > Servers**.
2. Under **Servers**, under **Local Site**, click the management server.
3. Under **Tasks**, click **Configure SecurID authentication**.
4. In the **Welcome to the Configure SecurID Authentication Wizard** panel, click **Next**.
5. In the **Qualification** panel of the **Configure SecurID Authentication Wizard** panel, read the prerequisites and verify that you meet them all.
6. Click **Next**.
7. In the **Upload RSA File** panel of the **Configure SecurID Authentication Wizard** panel, browse for the folder in which the `sdconf.rec` file resides.
You can also type the path name.
8. Click **Next**, and then click **Test** to test your configuration.
9. In the **Test Configuration** dialog box, type the user name and password for your SecurID, and then click **Test**.
It now authenticates successfully.

Adding Symantec Endpoint Protection Manager administrators who use RSA SecurID authentication

After you complete the previous procedures, you can add Symantec Endpoint Protection Manager administrators.

To add Symantec Endpoint Protection Manager administrators who use RSA SecurID authentication

1. Add an administrator account. See:
[Adding an administrator account and setting access rights](#)
2. On the **Authentication** tab, click RSA SecurID Authentication.
If this option is unavailable, review the configuration guidelines. See:
[Configuring RSA SecurID to authenticate Symantec Endpoint Protection Manager administrators](#)

3. Click **OK**.

You can also change an existing administrator account to use RSA SecurID authentication, though this practice is not recommended, especially for default administrator account, admin. If you provide invalid information when you edit an existing user, it is more difficult to recover that user.

However, if you modify an existing administrator account, in the **Confirm Change** dialog box, type the password that you use to log on to Symantec Endpoint Protection Manager, and then click **OK**.

When you switch between authentication methods, you must type the administrator account's password. See:

[Choosing the authentication method for administrator accounts](#)

Configuring two-factor authentication with Symantec VIP

If you use Symantec VIP two-factor authentication in your environment, you can configure Symantec Endpoint Protection Manager administrators to authenticate with it.

Two-factor authentication adds an extra layer of security to the logon process. When two-factor authentication is enabled, you must provide a unique, one-time verification code when you log on, in addition to a password. You can receive the code by voice, text, or with the free Symantec VIP Access app. This app is recommended because it is the most secure and it is easy to use. For a quick overview of Symantec VIP, see:

[Symantec VIP: Enterprise-grade authentication made easy for everyone](#)

You manage the individual two-factor authentication settings for each individual administrator that uses Symantec Endpoint Protection Manager Authentication. Administrators that authenticate with RSA SecurID or Directory authentication cannot use two-factor authentication.

NOTE

Two-factor authentication is not supported over IPv6, or in a FIPS-enabled environment.

To configure Symantec Endpoint Protection Manager for two-factor authentication with Symantec VIP

1. In the console, click **Admin > Servers**, and then click the local server name.
2. Under **Tasks**, click **Configure VIP authentication**.
3. Browse to the PKCS keystore file to select it, enter the keystore's password, and then click **OK**.
The certificate automatically propagates to other Symantec Endpoint Protection Manager consoles in the same site without the need for replication. You do not need to manually add the certificate to each Symantec Endpoint Protection Manager on the site.
To propagate the certificate to a Symantec Endpoint Protection Manager on a different site, the sites must be replication partners.

To configure the administrator for two-factor authentication with Symantec VIP

1. Verify that the Symantec Endpoint Protection Manager administrator has a corresponding user name on the Symantec VIP Manager that matches exactly, including case sensitivity. The passwords for the two user names do not have to match.
Consult Symantec VIP Manager documentation for how to configure a user name. See:
[Symantec VIP Access Manager 3.0 Administrator's Guide](#)
2. In the console, click **Admin > Servers > Administrators**.
3. Select an existing administrator, and then click **Edit the administrator**.
You can also add a new administrator to configure.
4. On the **Authentication** tab, click **Enable two-factor authentication using VIP**.

Configuring authentication with smart cards

In 14.2 or later, administrators who work for U.S. Federal Agencies can log on to Symantec Endpoint Protection Manager (SEPM) using a smart card.

To set up smart card authentication, the administrator must perform the following steps:

- [Step 1: Import the root and intermediate certificates into Symantec Endpoint Protection Manager](#)
- [Step 2: Import the certificate revocation list \(CRL\) \(required for dark networks\)](#)
- [Step 3: Add an administrator account and register the smart card](#)
- [Step 4: Log on to Symantec Endpoint Protection Manager using a smart card](#)

About smart cards

United States Federal Agencies require the use of smart card authentication to comply with [Homeland Security Presidential Directive 12](#) requirements. A U.S. Federal smart card contains the necessary data that grants the cardholder access to Federal facilities and information systems. This access ensures appropriate levels of security for all applicable Federal applications.

Card readers are often built into keyboards and laptops, but external USB readers are also supported. Check with the manufacturer for any applicable driver requirements.

Symantec Endpoint Protection Manager authenticates administrators who use the following types of smart cards:

- Personal identity verification (PIV) card, such as IDEMIA and Gemalto (for civilians)
- Common Access Card (CAC) (for military personnel)

Symantec Endpoint Protection Manager does not support smart cards in FIPS mode or smart cards that are signed using RSASSA-PSS. Symantec tests each release against the smart card sample pack available from NIST.

Step 1: Import the root and intermediate certificates into Symantec Endpoint Protection Manager

You must import the root certificates and/or intermediate certificates to use for the root of trust. This step establishes the root certification that is used for the verification of smart card sign-on. You can import multiple root certificates and intermediate certificates.

All the root files and intermediate files must be present on the Symantec Endpoint Protection Manager computer, and the intermediate certificate should be in the same chain as the root. Otherwise, administrators cannot log on.

To import the root certificates and intermediate certificates into Symantec Endpoint Protection Manager

1. In the console, click **Admin > Servers**, and then select the local management server name.
2. Under **Tasks**, click **Configure Smart Card Authentication**.
3. In the **Specify the paths for the root and/or intermediate certificate files** text box, browse to one or more certificate files, and then click **OK**.
Select all the certificate files that you need to establish trust. To select multiple files, press **Ctrl**.
4. Click **OK**.
5. Restart the Symantec Endpoint Protection Manager service. See:
[Stopping and starting the management server service](#)

Step 2: Import the certificate revocation list (CRL) and perform the revocation check (optional; required for dark networks)

If a management server does not have internet access, you must configure it to check for the CRL file on the management server computer instead. Without this check, administrators can still log on, but the management server cannot check the CRL file, which can cause security issues.

To import the certificate revocation list (CRL) into the management server

1. In the console, click **Admin > Servers**, and then select the local management server name.
2. Under **Tasks**, click **Configure Smart Card Authentication**.
3. In the **Specify the paths for the certificate revocation lists** text box, browse to one or more .crl or .pem files, and then click **OK**.
Select all of the certificate files that you need to check for revocation. To select multiple files, press **Ctrl**.
4. Click **OK**.

To bypass certificate validation

Because administrators logging on in a dark network cannot access the network, you must allow these administrators to connect regardless of the certificate in use. To allow the connection, bypass the certificate validation.

1. On the management server, open the following file: <Symantec Endpoint Protection Manager installation path>\tomcat\etc\conf.properties
2. In the conf.properties file, add smartcard.cert.revocation.ocsp.crl.dp.enabled=false and save the file.
3. Restart the management server service. See:
[Stopping and starting the management server service](#)

Step 3: Add an administrator account and register the smart card

This step imports the administrator's certificate, which is matched against their smart cards on SEPM logon.

- Smart card authentication requires a certificate and key pair that is used to verify that the PIV credential:
 - Was issued by an authorized entity.
 - Has not expired.
 - Has not been revoked and is in the same chain as the certificates that you imported in Step 1.
- The PIV credential also identifies that the administrator is the same individual who it was issued to.

This step also ensures that the administrator must enter a user name, insert the card, and enter the smart card pin to log on to Symantec Endpoint Protection Manager. The administrator does not need to enter a Symantec Endpoint Protection Manager password.

Smart card authentication is not supported over IPv6.

NOTE

Follow this step for each administrator who uses a smart card to log on to Symantec Endpoint Protection Manager.

To add an administrator account and register the smart card

1. In the console, click **Admin > Servers > Administrators**.
2. Add a new administrator or edit an existing administrator. See:
[Adding an administrator account and setting access rights](#)
3. On the **Authentication** tab, click **Enable smart card authentication**.
4. Browse to the authentication certificate file for the PIV card or CAC for that administrator, and then click **OK**.
5. In the **Confirm Change** dialog box, type the administrator password, and then click **OK**.

Step 4: Log on to Symantec Endpoint Protection Manager using a smart card

The Java console and web console support smart card authentication. The RMM console and the REST API do not support smart card authentication.

Before you log on, insert the card into a smart card reader. Type your PIN either before or after you log on, depending on which console you use.

The smart card must always be inserted into the reader while the smart card administrator is logged on and using the management server.

NOTE

If you run SEPM on a virtual machine, Symantec recommends the Windows Remote Desktop. If you use VMware ESXI, use the VMware Remote Console.

To log on to the Symantec Endpoint Protection Manager Java console

To log on to the Java console with the Gemalto IDPrime smart cards, you must install the Thales SafeNet driver.

1. Log on to the Symantec Endpoint Protection Manager Java console. See: [Logging on to the Symantec Endpoint Protection Manager console](#)
2. After the Symantec Endpoint Protection Manager logon screen appears, click **Options >>**, check **Log on with a smart card**, type your user name, and then click **Log On**.
3. Type the smart card PIN number, and then click **OK**.



The Symantec Endpoint Protection Manager console appears.

To log on to the Symantec Endpoint Protection Manager web console

Symantec recommends the following best practices:

- To use the web console, you may need to install the driver for the smart card manufacturer that your organization uses.
- Make sure that the intermediate or leaf certificate has not expired. When the browser prompts you to select a certificate in this task, an expired certificate does not appear in the list. The SEPM web console does not appear and you cannot log on.
- Most modern browsers support smart card login.
- For security reasons, after the administrator removes the smart card from the reader, the administrator should log off the web console immediately.

1. Open a supported web browser and type the following address in the address box:

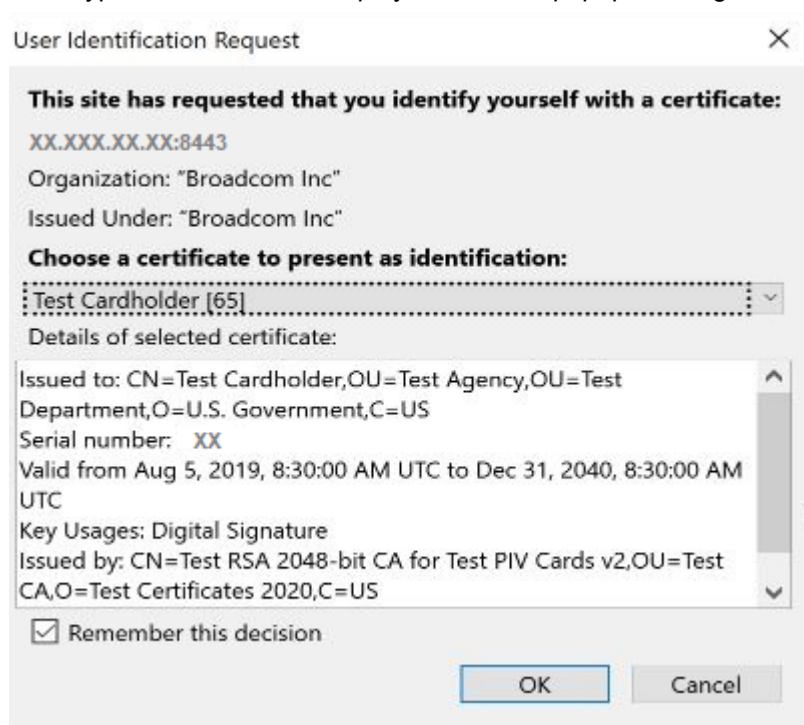
`http://<SEPMServer>:9090/`

Where **<SEPMServer>** is the host name or IP address of the management server.

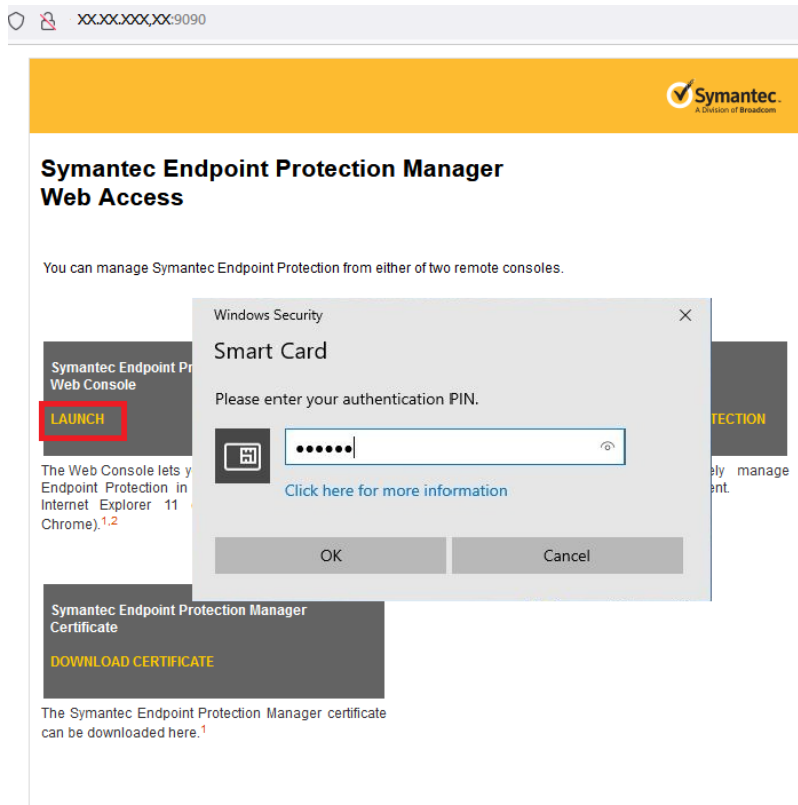
2. Under **Symantec Endpoint Protection Manager Web Console**, click **Launch**.

If one of the following popup messages appears after you log on to the console, make sure that you select the correct smart card certificate (leaf certificate) to trust. Otherwise, the web console does not appear.

Each type of web browser displays a different popup message.



3. In the **Windows Security Smart Card** logon screen, type your PIN number, and then click **OK**.



4. In the **Symantec Endpoint Protection Manager** logon screen, click **Options >>**, check **Log on with a smart card**, type your user name, and then click **Log On**.
A domain administrator must add the specific domain when logging in even if it is the default domain.

The screenshot shows the Symantec Endpoint Protection Manager logon screen. It has an orange header with the Symantec logo. Below the header, the Symantec logo is displayed next to the title "Symantec Endpoint Protection Manager". There are two input fields: "User name:" with the text "admin" and "Domain:". Below the "Domain:" field, there is a checkbox labeled "Log on with a smart card" which is checked. At the bottom, there are three buttons: "Log On" (orange), "Exit" (gray), and "Options <<" (gray). At the very bottom, there is a copyright notice: "Copyright © 2022 Broadcom. All Rights Reserved." and a paragraph of text: "The term 'Broadcom' refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, CA Technologies, the CA technologies logo, and Symantec are among the trademarks of Broadcom."

You may see:

- Another message to select the correct intermediate certificate. Select the same certificate that you selected before.
 - The smart card logon screen may appear a second time. Type the PIN number.
- The Symantec Endpoint Protection Manager console appears.

Using smart cards for multiple management servers and multiple sites

If you have multiple management servers or perform replication in your environment, you configure smart card authentication once. Replication for smart cards follows the same process as the policies.

To share certificates among multiple management servers within a single site

1. Configure smart card authentication on one management server in the site.
Wait 5 minutes until the other management servers that share the database are updated.
2. Restart all management servers.

To share certificates among multiple management servers across multiple sites

1. Configure smart card authentication on one management server in one site.
2. Replicate data between all sites.
Wait 5 minutes until the other management servers from the remote sites are updated.
3. Restart all management servers on all sites.

To confirm that each management server successfully replicated the certificate

1. Go to **Monitors > Logs**.
2. In the **log type** drop-down list, select **System > Server Activity**, and then click **View Log**.
3. In the **Event type** column, look for **Remote file download successful**.

Restoring the smart card configuration

If you misconfigured the smart card authentication, you can reset your current smartcard configuration back to the default behavior.

To restore the default smartcard configuration

1. Stop the Symantec Endpoint Protection Manager service.
2. Open the following files: `<SEPM installation directory>\apache\conf\ssl\smartCard.pem` and `<SEPM installation directory>\apache\conf\ssl\CRL.pem`
3. Remove all the certificate entries in these files except the first entry, and save the files.
4. Restart the Symantec Endpoint Protection Manager service.
SEPM should be back to its default state with no intermediate or root certificates added and no CRLs configured.

Testing directory server authentication for an administrator account

You can check that an Active Directory or LDAP server authenticates the user name and password for an administrator account that you create. The check evaluates whether you added the user name and password correctly, and whether or not the account name exists on the directory server.

You use the same user name and password for an administrator account in Symantec Endpoint Protection Manager as you do in the directory server. When the administrator logs on to the management server, the directory server authenticates the administrator's user name and password. The management server uses the directory server configuration that you added to search for the account on the directory server.

You can also check whether an Active Directory or LDAP server authenticates an administrator account with no user name and password. An account with no user name or password is anonymous access. You should create an

administrator account with anonymous access so that the administrators are never locked out if the password changes on the directory server.

NOTE

In Windows 2003 Active Directory server, anonymous authentication is disabled by default. Therefore, when you add a directory server without a user name to an administrator account and click **Check Account**, an **Account Authentication Failed** error message appears. To work around this issue, create two directory server entries, one for testing, and one for anonymous access. The administrator can still log on to the management server using a valid user name and password.

Step 1: Add multiple directory server connections

To make testing easier for anonymous access, add at least two directory server entries. Use one entry to test the authentication, and the second entry to test anonymous access. These entries all use the same directory server with different configurations.

By default, most users reside in CN=Users unless moved to different organizational unit. Users in the LDAP directory server are created under CN=Users, DC=<sampldomain>, DC=local. To find out where a user resides in LDAP, use ADSIEdit.

Use the following information to set up the directory servers for this example:

- CN=John Smith
- OU=test
- DC=<sampldomain>
- DC=local

The example uses the default Active Directory LDAP (389) but can also use Secure LDAP (636).

To add multiple directory server connections

1. To add the directory server connections to check Active Directory and LDAP server authentication, on the console, click **Admin > Servers**, select the default server, and click **Edit the server properties**.
2. On the **Directory Servers** tab, click **Add**.
3. On the **General** tab, add the following directory server configurations, and then click **OK**.

Directory 1	• Name: <sampldomain> Active Directory • Server Type: Active Directory • Server IP Address or Name: server01.<sampldomain>.local • User Name: <sampldomain>\administrator • Password: <directory server password>
Directory 2	• Name: <sampldomain> LDAP with User Name • Server Type: LDAP • Server IP Address or Name: server01.<sampldomain>.local • LDAP Port: 389 • LDAP BaseDN: DC=<sampldomain>, DC=local • User Name: <sampldomain>\administrator • Password: <directory server password>

Directory 3	• Name: <sampldomain> LDAP without User Name • Server Type: LDAP • Server IP Address or Name: server01.<sampldomain>.local • LDAP Port: 389 • LDAP BaseDN: <empty> Leave this field empty when you use anonymous access. • User Name: <empty> • Password: <empty> After you click OK, a warning appears. But the directory server is valid. When you try to add a BaseDN without a user name and password, the warning appears.
-------------	---

Step 2: Add multiple administrator accounts

You add multiple system administrator accounts. The account for anonymous access does not have a user name or password.

To add multiple administrator accounts

1. To add the administrator accounts using the directory server entries, on the console, click **Admin > Administrators**, and on the **General** tab, add the administrator accounts in the previous step. See:
 - [Adding an administrator account and setting access rights](#)
 - [Choosing the authentication method for administrator accounts](#)
2. After you add each administrator account and click the **Check Account** option, you see a message. In some cases, the message appears to invalidate the account information. The administrator can still log on to Symantec Endpoint Protection Manager, however.
3. On the **General** tab, enter the following information:

Administrator 1	• Name: <sampldomain> LDAP without User Name • Server Type: LDAP • Server IP Address or Name: server01.<sampldomain>.local • LDAP Port: 389 • LDAP BaseDN: <empty> Leave this field empty when you use anonymous access. • User Name: <empty> • Password: <empty> After you click OK, a warning appears. But the directory server is valid. When you try to add a BaseDN without a user name and password, the warning appears.
Administrator 2	• User Name: john • Full Name: John Smith • Email Address: john@<sampldomain>.local • On the Access Rights tab, click System Administrator. • On the Authentication tab, click Directory Authentication. In the Directory Server drop-down list, select <sampldomain> LDAP with User Name. In the Account Name field, type john. Click Check Account. The system administrator john cannot log on into Symantec Endpoint Protection Manager with directory authentication

Administrator 3	• User Name: john • Full Name: John Smith • Email Address: john@<sampldomain>.local • On the Access Rights tab, click System Administrator. • On the Authentication tab, click Directory Authentication. In the Directory Server drop-down list, select <sampldomain> LDAP with User Name. In the Account Name field, type John Smith. Click Check Account. The system administrator john can log on into Symantec Endpoint Protection Manager with directory authentication.
Administrator 4	• User Name: john • Full Name: John Smith • Email Address: john@<sampldomain>.local • On the Access Rights tab, click System Administrator. • On the Authentication tab, click Directory Authentication. In the Directory Server drop-down list, select <sampldomain> LDAP without User Name. In the Account Name field, type John Smith. Click Check Account. The account authentication fails, but the system administrator John Smith can log on to Symantec Endpoint Protection Manager.

More information

[Synchronizing Active Directory groups with the Symantec Endpoint Protection Manager \(SEPM\)](#)

Configuring Okta for the LDAP server with multifactor authentication (14.3 RU8 or later)

If your organization already uses Okta integration for secure access, you can use Okta instead of using Symantec VIP to authenticate an administrator account.

Multifactor authentication adds an extra layer of security to the logon process. When administrators log on, they must either acknowledge a notification or provide a unique, one-time token.

For an overview of Symantec VIP, see: [Configuring two-factor authentication with Symantec VIP](#)

Step 1: Configure the LDAP connection in the Symantec Endpoint Protection Manager

First set up an LDAP connection between the Symantec Endpoint Protection Manager and your company's Okta server, with an automatic push notification.

To configure the LDAP connection in the Symantec Endpoint Protection

1. In the console, add an administrator account.
[Adding an administrator account and setting access rights](#)
2. On the **Authentication** tab, select **Directory Authentication > Directory Servers**.
3. In the **Directory Servers** dialog box, click **Add**.
4. In the **Add Directory Server** dialog box > **General** tab, add the following items:

-
- **Name:** <optionalname>
 - **Server Type:** LDAP
 - **Server Type Address or Name:** yourcompany.ldap.okta.com
 - **LDAP Port:** 636
 - **LDAP BaseDN:** ou=users,dc=<yourcompany>,dc=okta,dc=<top-leveldomain>. For example:
ou=users,dc=mycompany,dc=okta,dc=com
 - **User Name:** uid=<user@yourcompany.domain>,dc=<LDAP server name>,dc=<top-level domain name>. For example: uid=kg123456@mycompany.com,dc=mycompany,dc=okta,dc=com
 - **Password:** Administrator password for Okta.
5. Click **OK > OK**.
 6. On the **Authentication** tab, under **Directory Authentication**, add the following information:
 - **Directory Server:** <optionalname>
 - **Account Name:** For example: uid=kg123456@mycompany.com,dc=mycompany,dc=okta,dc=com
 7. Click **OK**.

Step 2: Logging on to the Symantec Endpoint Protection Manager using Okta Verify

Logging on to Symantec Endpoint Protection Manager depends on how your Okta administrator configured Okta Verify. The Symantec Endpoint Protection Manager administrator can log on:

- Automatically, without any notifications.
- By adding a password to acknowledge a push notification or add a multifactor password.

More information:

- [Configure an Okta sign-on policy](#)
- [Use multifactor authentication with the LDAP Interface](#)

To log on to the Symantec Endpoint Protection Manager console using Okta Verify automatic push

1. In the Symantec Endpoint Protection Manager logon screen > **Password** field, the administrator types their normal user password, and then clicks **OK**.
2. When a push notification appears, the administrator needs to approve the push.
The LDAP authentication completes and the Symantec Endpoint Protection Manager opens.

To log on to the Symantec Endpoint Protection Manager console using Okta Verify without an automatic push

For this logon configuration, the Okta administrator requires the administrator to either acknowledge a push notification or add a multifactor token.

1. In the Symantec Endpoint Protection Manager logon screen > **Password** field, the administrator types: one of the following options, and then clicks **OK**:
 - a. For a push notification: <password>,push
 - b. For a token: <password,MFAtoken>
For example, administrators enter: password, 123456, where *password* is the admin user password, and *123456* is the Okta Verify passcode.

Resetting a forgotten Symantec Endpoint Protection Manager password

If you have a system administrator account, you can reset your own password and allow other administrators to reset their own passwords.

To reset a lost password, make sure that the following items are enabled:

- Administrators can reset their own passwords. See:

[Displaying the Forgot your password link so that administrators can reset lost passwords](#)

- The **Forgot your password?** link is set to appear on the management server logon screen. By default, this link appears. See:

[Displaying the Remember my user name and check boxes on the logon screen](#)

- The mail server must be configured so that the mail server sends the notification.
To troubleshoot Symantec Endpoint Protection Manager email failure, see:
 - [Sending test email messages fails in Endpoint Protection Manager console](#)
 - [Establishing communication between the management server and email servers](#)

Use this method for the administrator accounts that authenticate by using Symantec Management Server authentication but not by either RSA SecurID authentication or directory authentication.

NOTE

In 14.2 and later, the password must contain at least 8 characters and fewer than 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character ["/ \ [] : ; | = , + * ? < >].

In 14.3 RU5 and later, the password must contain at least 8 characters and fewer than 1024 characters. You can use additional characters and a space. You can set the management server to require unique passwords.

[Enforcing a secure password for administrators and client users](#)

For more information, see:

[Choosing the authentication method for administrator accounts](#)

If you do not know the recipient's email address, see: [Finding out the Symantec Endpoint Protection Manager administrator email address](#)

To reset a forgotten Symantec Endpoint Protection Manager password

1. On the management server computer, click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager**.

By default, the **Forgot your password?** link appears on the management server logon screen.

2. In the **Logon** screen, click **Forgot your password?**
3. In the **Forgot Password** dialog box, type the user name for the account for which to reset the password.

For domain administrators and limited administrators, type the domain name for the account. If you did not set up domains, leave the domain field blank.

4. Click **Temporary Password**.

The administrator receives an email that contains a link to activate a temporary password. An administrator can request a temporary password from the management console only once per minute. For security reasons, the management server does not verify the entries.

5. The administrator must change the temporary password immediately after logging on.

To verify whether the administrator successfully reset the password, check that the administrator received the email message. See:

[Changing the password for an administrator account or the default database](#)

When you cannot reset your password

If you cannot recover your administrator password with the **Forgot your password?** functionality, Symantec cannot assist with the recovery of your password. You must reconfigure the Symantec Endpoint Protection Manager and database without a database backup. This procedure overwrites the previous management server and database settings and

enables you to recreate a new password. Therefore, it is critical that you configure your email settings correctly when you set up the management server and when you audit administrator account information. See:

- [Restoring the database](#)
- [Reinstalling or reconfiguring Symantec Endpoint Protection Manager.](#)

Displaying the Forgot your password link so that administrators can reset lost passwords

If you have a system administrator account, you can enable other administrators to reset their forgotten passwords. You enable a **Forgot your password?** link on the Symantec Endpoint Protection Manager logon screen so that administrators can request a temporary password.

To allow administrators to reset forgotten passwords

1. In the console, click **Admin**.
2. On the **Admin** page, click **Servers**.
3. Under **Servers**, select the local site.
You control this setting only for the local site.
4. Click **Edit Site Properties**.
5. On the **Passwords** tab, check **Allow administrators to reset the passwords**.
6. Click **OK**.

More information

- [Resetting a forgotten Symantec Endpoint Protection Manager password](#)
- [Displaying the Remember my user name and check boxes on the logon screen](#)

Account name and password requirements for Symantec Endpoint Protection Manager

Follow the allowed length and character requirements for the different account names and passwords that you need to administer Symantec Endpoint Protection Manager (SEPM).

The following requirements are enforced.

Table 157: Symantec Endpoint Protection Manager account name and password requirements

Component	Requirements
Symantec Endpoint Protection Manager administrator accounts	• User name: – No more than 20 characters allowed. – The following characters are not allowed: " / \ [] : ; = , + * ? < > • Password: – If you install with a SQL Server database, all characters are allowed. However, you can use no more than 256 characters, and no fewer than 6 characters. – If you install with the default database: • In 14.3 RU5 or later, the password can contain from 8 characters to 1024 characters. In addition, you can configure whether or not to require letters and numbers, unique passwords and a password reuse limit. You can use spaces. For more information, see: Enforcing a secure password for administrators and client users • In 14.3 RU4 or earlier, the password can contain from 6 and 30 characters. You cannot use spaces and the following characters are not allowed: \ " ; The same user name and password are used for the administrator account and for the SEPM with the default database. There are separate requirements for the Symantec Endpoint Protection Manager with a SQL Server database configuration.
SQL Server authentication	• SQL Server administrator name (DBA user): – Cannot be blank. – You can use lowercase and uppercase letters, numerals, and the following special characters: & _ # \$ • Other special characters are not allowed. – The default value in the SEPM is sa (the default built-in administrator account for SQL Server). You can specify any account that has Server Administrator access rights. • SQL Server administrator password (DBA password): – No more than 128 characters allowed (79 characters for the Windows authentication method). – All characters are allowed, including high ASCII or double-byte characters, with the following limitations based on Symantec Endpoint Protection Manager version and authentication method: • Earlier than 14.2 RU1: The following characters are not allowed for SQL Authentication or Windows Authentication: " [] { } () , ; ? * ! @ ; • 14.2 RU1 and later: For first-time SEPM installations, the following characters are allowed for Windows Authentication but not for SQLServer Authentication: " [] { } () , ; ? * ! @ ; . • If you reconfigure SEPM, the following characters are not allowed: / " < > – Refer to the Microsoft documentation for recommendations about setting the DBA password. • This password is set on your SQL Server computer. • You do not create it on the SEPM; you only provide it. • SQL Server Database Administrator with Windows authentication: – Uses the existing Windows user name and password for the database server. – The following characters are not allowed for the Windows Authentication password: < > / " • SQL Server SEP database name: – Cannot be blank. – Only the following characters are allowed: lowercase and uppercase letters, numerals, and the special characters & _ # \$ • Other special characters are not allowed. – The default value for the Symantec Endpoint Protection database is sem5 (the same value as the database user name).

Component	Requirements
SEPM with default database (SQL Server Express or embedded)	• Database user name (User): – No more than 128 characters allowed; cannot be blank. – Only the following characters are allowed: lowercase and uppercase letters, numerals, and the special characters: ~ # % _ + = : . • The following special characters are not allowed: ` ! @ ' \$ ^ & * () - { } [] " \ / < ; > , ? – The default value for the Symantec Endpoint Protection database user name is sem5. • SEPM database user password (Password): – No more than 128 characters allowed; cannot be blank. – Only lowercase and uppercase letters, numerals, and the following special characters are allowed: ~ # % _ + = : . / • The following special characters are not allowed: ! @ * () { } [] ; , ?
Encryption password	• The Management Server Configuration Wizard can generate this password for you. • If you choose to set your own password, it can contain from 8 characters to 1024 characters (14.3 RU5 or later) or from 6 to 32 characters (14.3 RU4 and earlier). All characters are allowed.
Symantec Endpoint Protection Manager group names	• A group name can contain no more than 990 characters. • The full path of the group name can contain no more than 1000 characters. • The following characters are not allowed: " / \ * ? < > : &
Symantec Endpoint Protection Manager domain names	• A domain name can contain no more than 256 characters, and it cannot be blank. • The following characters are not allowed: " / \ [] : ; = , + * ? < >
Symantec Endpoint Protection Manager site names	• A site name can contain no more than 60 characters, and it cannot be blank. • All characters are allowed.

Changing the password for an administrator account or the default database

Changing the password for an administrator account

You need to change the password for your account or another administrator's account if the password is forgotten, lost, or compromised.

The following rules apply to changing passwords:

- System administrators can change the password for all administrators.
- Domain administrators can change the password for other domain administrators and limited administrators within the same domain.
- Limited administrators can change their own passwords only.

If you change the password to fix an administrator account lockout, the administrator must still wait for the lockout period to expire.

NOTE

In 14.2 or later, the password must contain from 8 characters and 16 characters. It must include at least one lowercase letter [a-z], one uppercase letter [A-Z], one numeric character [0-9], and one special character such as ["/\ [] : ; | = , + * ? < >] @].

In 14.3 RU5, the password must contain from 8 characters and 1024 characters. In addition, you can configure whether or not to require letters and numbers, unique passwords and a password reuse limit. See:

[Enforcing a secure password for administrators and client users](#)

For more information, see:

Unlocking an administrator's account after too many logon attempts

To change the password for an administrator account

1. In the console, click **Admin > Administrators**.
2. Under **Administrators**, select the administrator account, and then click **Change password**. Press **F1** to see the password restrictions.
3. Type both your password and the administrator's new password.
4. Click **Change**. See:
 - [Resetting a forgotten Symantec Endpoint Protection Manager](#)
 - [Displaying the Forgot your password? link so that administrators can reset lost passwords](#)

Changing the default database password

When you configure the management server and select the default database (Microsoft SQL Server Express or embedded (14.3 MPx and earlier), the password you enter for the default administrator account, `admin`, also becomes the database password. If you change the default administrator's password, the database password does not change automatically. You can change the database password by rerunning the Management Server Configuration Wizard and reconfiguring Symantec Endpoint Protection Manager.

To change the default database password

1. On the Windows **Start** menu, navigate to **Symantec Endpoint Protection Manager > Management Server Configuration Wizard**.
2. Click **Reconfigure the management server**, and then click **Next > Next**. See: [Reinstalling or reconfiguring Symantec Endpoint Protection Manager password](#)
3. Click one of the following options and then click **Change the database administrator password** and type the new password.
 - Click **Default SQL Server Express database** (14.3 RU1 and later).
 - Click **Default Embedded database** (14.3 MPx and earlier).
4. Follow the instructions in each panel to finish the configuration.

Enforcing a secure password for administrators and client users

In 14.3 RU5 and later, Symantec Endpoint Protection Manager (SEPM) lets system administrators create complex passwords for administrators that protect your computers against brute force attacks. You can set the password requirements to meet the password policy guidelines of your organization. These settings override the default SEPM password requirements. If you want to continue to use the default SEPM password requirements, disable the options below.

These password requirements apply across all domains and for all types of administrators (system, domain, and limited) and in the following situations:

- Configuring and changing administrator passwords
 - [Adding an administrator account and setting access rights](#)
 - [Changing the password for an administrator account or the default database](#)
- Configuring client passwords
 - [Password-protecting the Symantec Endpoint Protection client](#)

Review the following information:

- The administrator account for the default Microsoft SQL Server Express database or the Microsoft SQL Server database has separate password requirements.
- The level of complexity must also meet Microsoft SQL Express password requirements and should be equally or more complex than the current SEPM requirements.
- When you first configured the management server in the Management Server Configuration Wizard, you could select the default installation or custom installation. If you selected the default installation, the password you entered is the same as the encryption password. If you now change the administrator's password, the encryption password does not change.
- When you upgrade from 14.3 RU4 or earlier, the existing passwords are still valid. However, the next time you configure a password, it must adhere to these stricter requirements.
- The password strength levels are stricter in 14.3 RU5 and later. For example, what was considered `Good` in RU4 and earlier is `Weak` in RU5.

For the password requirements, see:

[Account name and password requirements for Symantec Endpoint Protection Manager](#)

To enforce a secure password for administrators and client users

1. In the console, click **Admin > Administrators**.
2. Click **Configure password requirements**, and change the default values as needed.

Options	14.3 RU5 and later defaults	14.3 RU4 and earlier defaults
Uppercase letters [a-z], lowercase letters [A-Z], and numbers [0-9]	Enabled	Enabled - cannot disable
Special characters	~ ` # \$ % - _ + = : . ' ^ & / \ < > [] { and a space.	Same. The Create Admin User REST API does not support the space or the " ; \ special characters. (14.3 RU5 and earlier).
Minimum number of characters	8	8
Maximum number of characters	1024	16
Limit password reuse	Enabled	No restrictions
Number of unique passwords before an administrator can reuse a password	6	No restrictions
Maximum days before an administrator can reuse a password	90	No restrictions

3. Click **OK**.

Enabling Symantec Endpoint Protection Manager logon passwords to never expire

If you use Symantec Endpoint Protection Manager authentication, the default option for passwords is set to expire after 60 days.

You can display an option for administrators to use a password that never expires. This option is disabled by default to increase security, so you must enable it first. After you enable the option, the option appears on the **Authentication** tab for an administrator account.

To enable Symantec Endpoint Protection Manager logon passwords to never expire

-
1. In the console, click **Admin**.
 2. On the **Admin** page, click **Domains**.
 3. Under **Domains**, select the domain for which to allow administrators to save logon credentials.
 4. Click **Edit Domain Properties**.
 5. On the **Passwords** tab, click **Allow never expiring passwords for administrators**.
 6. Click **OK**.
 7. Click **Admin > Administrators**, and open the administrator account.
 8. On the **Authentication** tab, click **Password never expires**, and then click **OK**.

More information

- [Resetting a forgotten Symantec Endpoint Protection Manager password](#)
- [Unlocking an administrator's account after too many logon attempts](#)

Displaying a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console

You can create and display a customizable message that all administrators see before they can log on to the console. The main purpose is to display a legal notice to tell the administrators that they are about to log on to a proprietary computer.

The message appears in the console after administrators type their user name and password and click **Log On**. After administrators have read the message, they can acknowledge the notice and click **OK**, which logs on the administrators. If administrators click **Cancel**, the logon process is canceled, and the administrator is taken back to the logon window.

The message also appears if the administrator runs the reporting functions from a standalone web browser that is connected to the management server.

To display a message for administrators to see before logging on to the Symantec Endpoint Protection Manager console

1. In the console, click **Admin**, and then click **Domains**.
2. Select the domain for which you want to add a logon banner.
3. Under **Tasks**, click **Edit Domain Properties**.
4. On the **Logon Banner** tab, check **Provide a legal notice to administrators when they log on to Symantec Endpoint Protection Manager**.
5. Type the banner title and text.
Click **Help** for more information.
6. Click **OK**.

More information

[Adding an administrator account and setting access rights](#)

Displaying the Remember my user name and Remember my password check boxes on the logon screen

A system administrator can enable the **Remember my user name** and **Remember my password** check boxes to appear on the Symantec Endpoint Protection Manager logon screen for another administrator account. The administrator's user name and password are prepopulated on the logon screen.

To display the Remember my user name and Remember my password check boxes on the logon screen

1. In the console, click **Admin**.
2. On the **Admin** page, click **Domains**.
3. Under **Domains**, select the domain for which to allow administrators to save logon credentials.
4. Click **Edit Domain Properties**.
5. On the **Passwords** tab, check **Allow users to save credentials when logging on**.
6. Click **OK**.

More information

[Resetting a forgotten Symantec Endpoint Protection Manager password](#)

Granting or blocking access to remote Symantec Endpoint Protection Manager consoles

By default, all consoles are granted access. Administrators can log on to the main console locally or remotely from any computer on the network.

You can secure a management console from remote connections by denying access to certain computers.

You may want to grant or deny access from the following types of users or computers:

- You should deny access to anyone on the Internet. Otherwise, the console is exposed to Internet attacks.
- You should deny access to limited administrators who use consoles on a different network than the network they manage.
- You should grant access to system administrators and IT administrators.
- You should grant access to lab computers, such as a computer that is used for testing.

In addition to globally granting or denying access, you can specify exceptions by IP address. If you grant access to all remote consoles, the management server denies access to the exceptions. Conversely, if you deny access to all remote consoles, you automatically grant access to the exceptions. When you create an exception, the computer that you specified must have a static IP address. You can also create an exception for a group of computers by specifying a subnet mask. For example, you may want to grant access in all areas that you manage. However, you may want to deny access to a console that is located in a public area.

To grant or deny access to a remote console

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, select the server for which you want to change the remote console access permission.
3. Under **Tasks**, click **Edit the server properties**.
4. On the **General** tab, click **Granted Access** or **Denied Access**.
5. If you want to specify IP addresses of the computers that are exempt from this console access permission, click **Add**.

Computers that you add become exceptions. If you click **Granted Access**, the computers that you specify are denied access. If you click **Denied Access**, the computers that you specify are granted access. You can create an exception for a single computer or a group of computers.

6. In the **Deny Console Access** dialog box, click one of the following options:
 - **Single Computer**
For one computer, type the IP address.
 - **Group of Computers**
For several computers, type both the IP address and the subnet mask for the group.

-
7. Click **OK**.

The computers now appear in the exceptions list. For each IP address and mask, its permission status appears.

If you change **Granted Access** to **Denied Access** or vice versa, all exceptions change as well. If you have created exceptions to deny access, they now have access.

8. Click **Edit All** to change the IP addresses or host names of those computers that appear on the exceptions list.

The **IP Address Editor** appears. The **IP Address Editor** is a text editor that lets you edit IP addresses and subnet masks.

9. Click **OK**.

10. When you finish adding exceptions to the list or editing the list, click **OK**.

More information

- [Adding an administrator account and setting access rights](#)
- [Logging on to the Symantec Endpoint Protection Manager console](#)

Unlocking an administrator account after too many logon attempts

Symantec Endpoint Protection Manager locks out an administrator for a certain length of time after multiple unsuccessful logon attempts. By default, the management server locks out an administrator for 15 minutes after five failed attempts.

You may want to lock an administrator account to block against the malicious attacks that use random user names and passwords to log on to the management server.

For added security, after the first lockout, the lockout interval doubles with each additional lockout. Symantec Endpoint Protection Manager reinstates the original lockout interval after a successful login occurs or after 24 hours pass since the first lockout. For example, if the original lockout interval is 15 minutes, the second lockout triggers a 30-minute lockout interval. The third lockout triggers a 60-minute lockout interval. If the first lockout occurs at 2:00 P.M. on Thursday, then the 24-hour period ends 2:00 P.M. Friday, and Symantec Endpoint Protection Manager resets the lockout interval to 15 minutes.

Disabling an administrator account from locking

You can disable the administrator account from locking, though this action does not unlock the account. You can also change the number of unsuccessful logon attempts and wait time that is allowed before the account is locked. A password change does not reset or otherwise affect the lockout interval.

To disable an administrator account from locking

1. In the console, click **Admin > Administrators**.
2. Under **Administrators**, select the administrator account that is locked.
3. Under **Tasks**, click **Edit the administrator**.
4. On the **General** tab, uncheck **Lock the account after the specified number of unsuccessful logon attempts**.

Unlocking an administrator account

The administrator can unlock their account in either one of the following ways:

- Use the reset account lock option.
- Wait for the specified time to pass.

To use the reset account lock option

1. In the console, click **Admin > Administrators**.

-
2. Under **Administrators**, select the administrator account and click **Reset Account Lock**.
The message `Administrator <name> is unlocked successfully` appears.

More information

- [Resetting a forgotten Symantec Endpoint Protection Manager password](#)
- [Changing the password for an administrator account or the default database](#)
- [Enabling Symantec Endpoint Protection Manager logon passwords to never expire](#)

Changing the timeout period for staying logged on to the Symantec Endpoint Protection Manager console

To help protect Symantec Endpoint Protection Manager, the console requires you to enter your user name and password again after one hour. To increase security, you can decrease the timeout period before you must log on to the management console again.

This logon timeout period applies to when you log on to the management console locally or through the remote Java console. The logon timeout period for the remote web console is based on the shortest timeout value that you define. For example, you set the **Site Properties** settings to 60 minutes, the Apache settings to 30 minutes, and the browser settings to 10 minutes. The console then times out after 10 minutes.

To change the timeout period

1. To change the timeout period for staying logged on to the Symantec Endpoint Protection Manager local or remote Java console, in the console, click **Admin**, and then click **Servers**.
2. Click **Local Site** or a remote site and click **Edit Site Properties**.
3. On the **General** tab, click the **Console Timeout** drop-down list and select one of the available options for length of time.
4. Click **OK**.
5. To change the timeout period in Apache Tomcat for staying logged on to the Symantec Endpoint Protection Manager remote web console, on the server that runs Symantec Endpoint Protection Manager, open the following file in a text editor:

```
Program Files\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties
```

6. Add the following line, if it is not present:

```
scm.web.timeout.minutes=timeout_value
```

The value `timeout_value` is the number of minutes of inactivity after which the console logs out. The maximum value is 60. A value of 0 has the same effect as not adding the line at all.

If this line is present, you can change the timeout value.

7. Save and close the file.
8. For your changes to take effect, open the Windows Services (services.msc) and restart the Symantec Endpoint Protection Manager service.
9. To change the timeout period in Internet Explorer for staying logged on to the Symantec Endpoint Protection Manager remote web console, follow the instructions in following the Microsoft article to change the registry key `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings`:

[How to change the default keep-alive time-out value in Internet Explorer](#)

10. To change the timeout period in Mozilla Firefox for staying logged on to the Symantec Endpoint Protection Manager remote web console, in the address bar, enter the following:

`about:config`

11. Click to acknowledge the warning.

12. Search for the following line:

`network.http.keep-alive.timeout`

13. Change the value (in seconds) to the one that you want. The default is 115.

NOTE

Google Chrome does not have configurable settings for the network timeout period.

More information

[Logging on to the Symantec Endpoint Protection Manager console](#)

About domains

When you install a management server, the Symantec Endpoint Protection Manager console includes one domain, which is called Default. Domains are a logical separation of data that is separate from the Symantec Endpoint Protection Manager infrastructure. A domain is a structural container in the console that you use to organize a hierarchy of groups, clients, computers, and policies. You set up additional domains to manage your network resources.

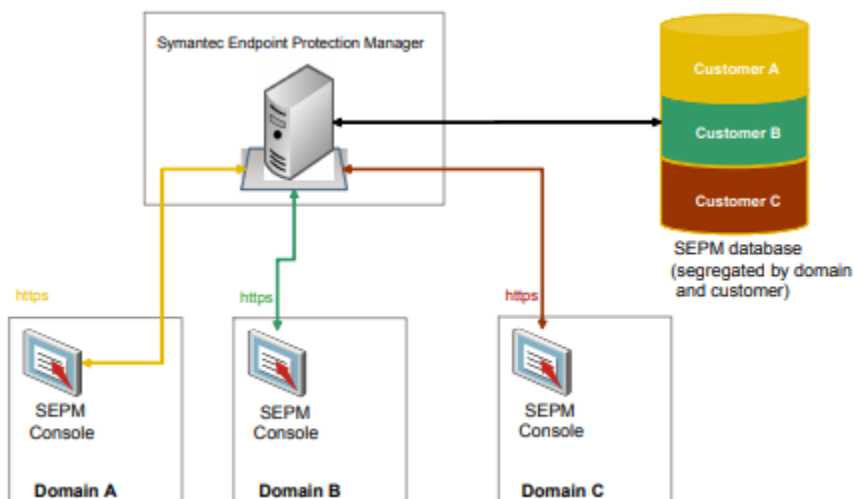
The primary purpose of domains is for managed service providers to build a single Symantec Endpoint Protection Manager infrastructure that services multiple customers.

NOTE

The domains in Symantec Endpoint Protection Manager are not equivalent to Windows domains or other network domains.

Each domain that you add shares the same management server and database, and it provides an additional instance of the console. All data in each domain is completely separate. This separation prevents administrators in one domain from viewing data in other domains. You can add an administrator account so that each domain has its own administrator. These administrators can view and manage only the contents of their own domain.

If your company is large, with sites in multiple regions, you may need to have a single view of management information. You can delegate administrative authority, physically separate security data, or have greater flexibility in how users, computers, and policies are organized. If you are a managed service provider (MSP), you may need to manage multiple independent companies, as well as Internet service providers. To meet these needs, you can create multiple domains. For example, you can create a separate domain for each country, region, or company.



When you add a domain, the domain is empty. You must set the domain to be the current domain. You then add administrators, groups, clients, computers, and policies to this domain.

You can copy policies from one domain to another. To copy policies between domains, you export the policy from the originating domain and you import the policy into the destination domain.

You can also move clients from one domain to another. To move clients between domains, the administrator of the old domain must delete the client from the client group. You then replace the Communication Settings file on the client with one from the new domain.

You can disable a domain if you no longer need it. Ensure that it is not set as the current domain when you attempt to disable it.

More information

- [Adding a domain](#)
- [Switching to the current domain](#)

Adding a domain

You create a domain to organize a hierarchy of groups, users, clients, and policies in your organization. For example, you may want to add domains to organize users by division.

NOTE

You can use a domain ID for disaster recovery. If all the management servers in your organization fail, you need to rebuild the management server by using the same ID as the old server. You can get the old domain ID from the sylink.xml file on any client.

To add a domain

1. In the console, click **Admin**.
2. On the **Admin** page, click **Domains**.
3. Under Tasks, click **Add Domain**.
4. In the Add Domain dialog box, type a domain name, an optional company name, and optional contact information.
5. If you want to add a domain ID, click **Advanced** and then type the value in the text box.
6. Click **OK**.

More information

Switching to the current domain

The default domain name is **Default**, and it is set as the current domain. When you add a new domain in the Symantec Endpoint Protection Manager console, the domain is empty. To add groups, clients, policies, and administrators to a new domain, you must first set it as the current domain. When a domain is designated as the current domain, the text **Current Domain** follows the domain name in the title. If you have many domains, you must scroll through the **Domains** list to display which domain is the current one.

If you logged on to the console as a system administrator, you can see all domains no matter which domain is the current one. However, you can only see the administrators and limited administrators that were created in the current domain. If you logged on to the console as either an administrator or a limited administrator, you only see the domain to which you have access.

If you remove the current domain, the management server logs you out. You can only remove a domain if it is not the current domain and not the only domain.

To switch to the current domain

1. In the console, click **Admin**.
2. On the **Admin** page, click **Domains**.
3. Under **Domains**, click the domain that you want to make the current domain.
4. Under **Tasks**, click **Administer Domain**.
5. In the Administer Domain dialog box, to confirm, click **Yes**.
6. Click **OK**.

More information

- [About domains](#)
- [Adding a domain](#)

How to update content and definitions on the clients

Update content including virus definitions, intrusion prevention signatures, and Host Integrity templates, among others.

By default, the Symantec Endpoint Protection Manager downloads content updates from the public Symantec LiveUpdate servers. Symantec Endpoint Protection clients then download these updates from the Symantec Endpoint Protection Manager. The content includes virus definitions, intrusion prevention signatures, and Host Integrity templates, among others.

NOTE

To update content on the Symantec Endpoint Protection Manager when it cannot access either the Internet or the LiveUpdate Administrator (LUA) server, you can download and install certified definitions using a .jdb file. Make sure you download and apply the correct .jdb file. For example, 14.3 RU6 definitions can apply to all clients from 14.3 RU0 through 14.3 RU6, but 14.3 RU7 definitions apply to 14.3 RU7 clients only.

You can create an automatic script that uses .jdb file name format, although Symantec may change the format. Do not create an automated script that unzips and copies the file names from inside of the .jdb.

[Download .jdb files to update definitions for Endpoint Protection Manager](#)

Table 158: Steps to update content on the Symantec Endpoint Protection clients

Task	Description
Make sure that the management server has the latest content from LiveUpdate (Recommended)	By default, LiveUpdate runs as part of the Symantec Endpoint Protection Manager installation. You may need to run LiveUpdate manually in the following situations: • You skipped LiveUpdate during installation. • You must run LiveUpdate to download the Host Integrity templates and intrusion prevention signatures. • You want to run LiveUpdate before the next scheduled update. For more information, see: Checking that Symantec Endpoint Protection Manager has the latest content Additionally, if you use replication, you can replicate content and policies between the local site and the partner site. See: How to install a second site for replication
Change how client computers get updates (Optional)	By default, Windows client computers get content updates from the management server. Other delivery methods include Group Update Providers, internal LiveUpdate servers, or third-party tool distribution. You may need to change the delivery method to support different client platforms, large numbers of clients, or network limitations. See: • Choose a distribution method to update content on clients • Choose a distribution method to update content on clients based on the platform
Change the LiveUpdate settings for the management server (Optional)	You can customize the frequency of LiveUpdate sessions, the protection components that are downloaded, and more. See: Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager
Reduce network overloads (Recommended)	If the management server receives too many concurrent requests for full definition packages from the clients, the network may become overloaded. You can mitigate the risk of these overloads, and stop clients from downloading full definitions. See: Mitigating network overloads for client update requests

Task	Description
Improve performance (Recommended)	To help mitigate the effect of downloads on network bandwidth, download content randomly so that not all clients get updates at the same time. See: • About randomization of simultaneous content downloads • Randomizing content downloads from the default management server or a Group Update Provider • Randomizing content downloads from a LiveUpdate server To mitigate the effect of downloads on client computers' performance, you can have the client computers download content updates when the client computers are idle. See: Configuring Windows client updates to run when client computers are idle
Let your endpoint users manage their own updates (Optional)	By default, users on the client computer can run LiveUpdate at any time. You can decide how much control to give your users over their content updates. See: Configuring the amount of control that users have over LiveUpdate You can also use an Intelligent Updater file on a client computer to update the definitions. See: Using Intelligent Updater files to update content on Symantec Endpoint Protection clients
Test engine updates before Symantec releases them (Optional)	Symantec releases engine updates on a quarterly basis. You can download the engine updates before they are released using a specific Symantec LiveUpdate server. You can then test the engine content before you roll out the content to your production environment. See: Testing engine updates before they release on Windows clients

More information

[Preparing unmanaged clients to receive updates from third-party distribution tools](#)

For information on LiveUpdate error codes, see: [LiveUpdate error codes \(Endpoint Protection/Endpoint Security\)](#)

Choose a distribution method to update content on clients

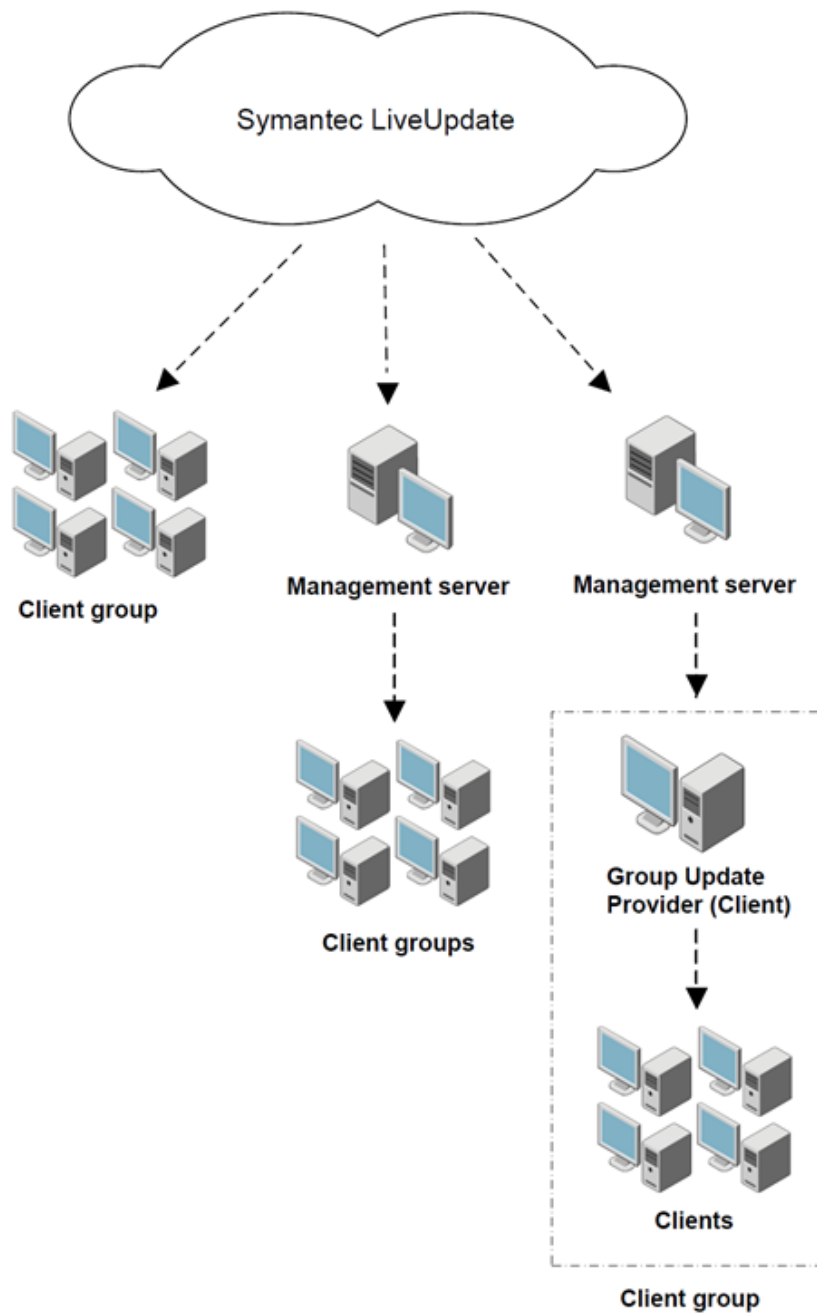
You may need to change the default update method to the clients, depending on the client platform, network configuration, number of clients, or your company's security policies and access policies.

Table 159: Content distribution methods and when to use them

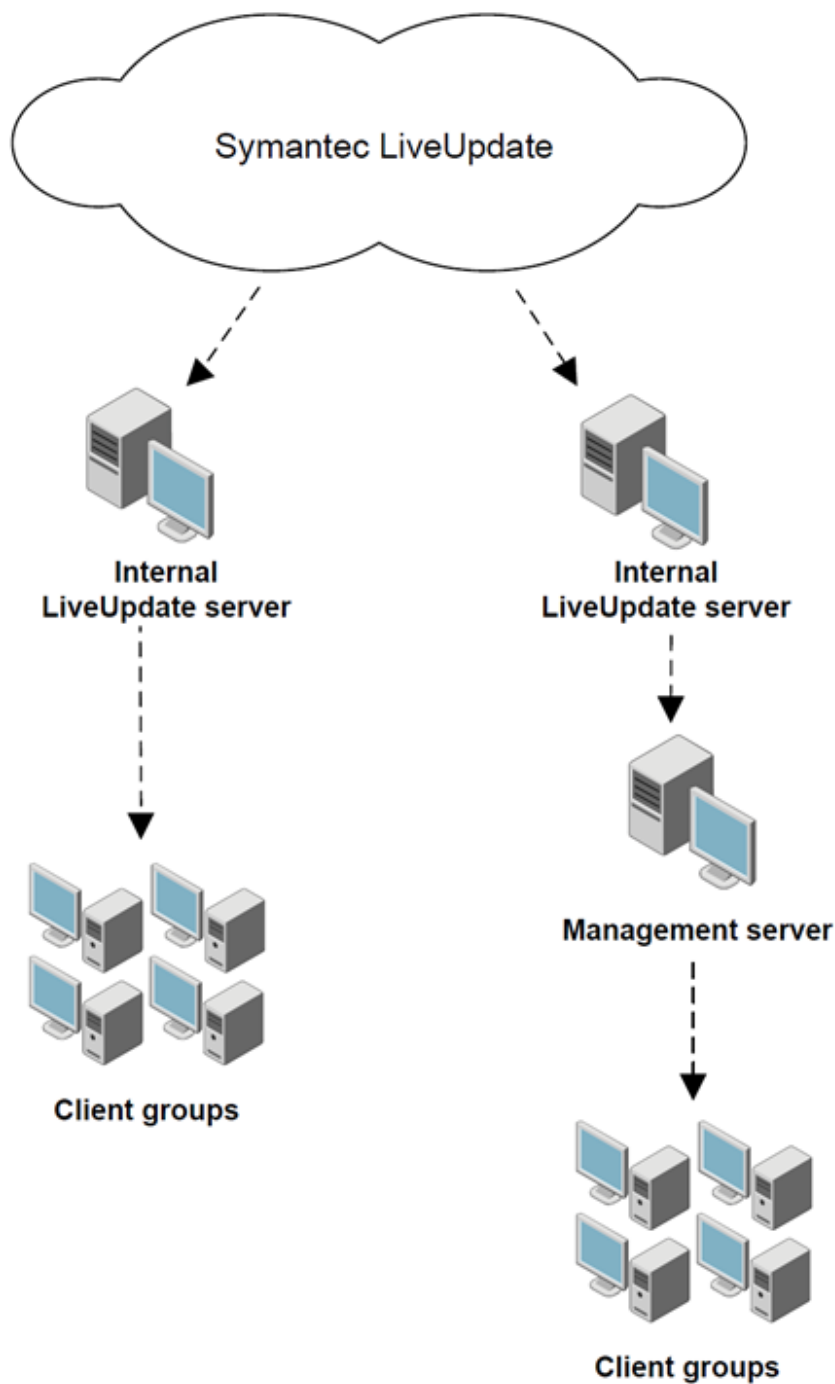
Method	Description	When to use it
Symantec Endpoint Protection Manager to client computers (default) (Windows, Mac, Linux)	The default management server automatically updates the client computers that it manages. You do not define the schedule for the updates from the management server to the clients. The clients download content from the management server based on the communication mode and heartbeat frequency. See: • Configuring clients to download content from the Symantec Endpoint Protection Manager • Updating policies and content on the client using push mode or pull mode	Symantec recommends that you use this method unless network constraints or your company's policies require an alternative. If you have a large number of clients or bandwidth issues, you might use this method, along with Group Update Providers. For Mac or Linux computers to receive content updates from the management server, you must configure the Apache web server. See: Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy
Group Update Provider to client computers (Windows only)	A Group Update Provider is a client computer that receives updates from a management server. The Group Update Provider then forwards the updates to the other client computers in the group. A Group Update Provider can update multiple groups. Group Update Providers can distribute all types of LiveUpdate content except client software updates. Group Update Providers also cannot be used to update policies.	A Group Update Provider lets you reduce the load on the management server, and is easier to configure than an internal LiveUpdate server. Use a Group Update Provider for groups at remote locations with minimal bandwidth. See: • Using Group Update Providers to distribute content to clients • Deciding whether or not to set up multiple sites and replication
Internal LiveUpdate server to client computers (Windows, Mac, Linux)	Client computers can download updates directly from an internal LiveUpdate server that receives its updates from a Symantec LiveUpdate server. If necessary, you can set up several internal LiveUpdate servers and distribute the list to client computers. You can change the download schedule from the LiveUpdate server to the management server. See: Configuring the LiveUpdate download schedule to client computers For more information about setting up an internal LiveUpdate server, see the <i>LiveUpdate Administrator User's Guide</i> at: Downloading LiveUpdate Administrator	An internal LiveUpdate server lets you reduce the load on the management server in very large networks. In smaller networks, consider whether Group Update Providers would meet your organization's needs. Consider using an internal LiveUpdate server in the following situations: • If you manage a large network (more than 10,000 clients) • If you manage Mac or Linux clients that should not connect to an external LiveUpdate server • If your organization deploys multiple Symantec products that also use LiveUpdate to distribute content to client computers Note: You should not install the management server and an internal LiveUpdate server on the same physical hardware or virtual machine. Installation on the same computer can result in significant server performance problems. For more information see: • LiveUpdate Administrator 2.x and Symantec Endpoint Protection Manager on the same computer • Configuring clients to download content from an internal LiveUpdate server

Method	Description	When to use it
External Symantec LiveUpdate server to client computers over the Internet (Windows, Mac, Linux)	Client computers can receive updates directly from a Symantec LiveUpdate server.	Use an external Symantec LiveUpdate server if you need to schedule when clients update content or if the available bandwidth between the Symantec Endpoint Protection Manager and the clients is limited. Symantec Endpoint Protection Manager and scheduled updates are enabled by default. With the default settings, clients always get updates from the management server unless management server is unresponsive for a long period of time. Note: Do not configure large numbers of managed, networked clients to pull updates from an external Symantec LiveUpdate server. This configuration consumes unnecessary bandwidth. For more information, see: Configuring clients to download content from an external LiveUpdate server
Third-party tool distribution (Windows only)	Third-party tools like Microsoft SMS let you distribute specific update files to clients.	This method lets you test update files before you distribute them. It may also make sense if you have a third-party tool distribution infrastructure in place. See: Distributing the content using third-party distribution tools
Intelligent Updater (Windows only)	Intelligent Updater files contain the virus and security risk content and intrusion prevention content that you can use to manually update clients. You can download the Intelligent Updater self-extracting files from the Symantec Web site.	You can use Intelligent Updater files if LiveUpdate is not available. See: Using Intelligent Updater files to update content on Symantec Endpoint Protection clients To update other kinds of content, you must set up and configure a management server to download and to stage the update files. See: Using third-party distribution tools to update client computers

The following figure shows an example distribution architecture for smaller networks.



The following figure shows an example distribution architecture for larger networks.



More information

- [Choose a distribution method to update content on clients based on the platform](#)
- [How to update content and definitions on the clients](#)
- [Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

Choose a distribution method to update content on clients based on the platform

The methods that you can use to distribute virus definitions and other content to the client computers depends on the client platform.

Table 160: Content distribution method based on Windows, Mac, and Linux clients

Platform	Method
Windows	By default, the Windows client gets content from the management server. Windows clients can also get updates from the following sources: • A LiveUpdate server (external or internal). See: – Configuring clients to download content from an internal LiveUpdate server – Configuring clients to download content from an external LiveUpdate server • An external LiveUpdate server (testing only). See: Testing engine updates before they release on Windows clients • A Group Update Provider. See: Using Group Update Providers to distribute content to clients • Third-party distribution tools. See: Distributing the content using third-party distribution tools • Intelligent Updater. See: Using Intelligent Updater files to update content on Symantec Endpoint Protection clients For more information, see: Choose a distribution method to update content on clients For Windows clients, you can also customize the following settings: • The content types that the client receives • Whether the client can get definitions from multiple sources • Whether the client can get smaller packages (deltas) from LiveUpdate if the management server can provide only full definition packages Full definition packages are very large. Too many downloads of full packages can overload your network. Deltas are typically much smaller, and affect your network bandwidth much less. See: Mitigating network overloads for client update requests
Mac or Linux	• A LiveUpdate server (external or internal) • An Apache Web server that you configure as a reverse proxy. See: Enabling Mac or Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy

More information

- [Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)
- [About the types of content that LiveUpdate downloads](#)
- [How to update content and definitions on the clients](#)

Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager

When you configure the management server to download LiveUpdate content, you have to make a number of decisions. When you download content to Symantec Endpoint Protection Manager, you download the content for all the management servers in the site.

Decisions to make about downloading content

Table 161: Decisions about content downloads

Decision	Description
What LiveUpdate server should serve the content to the site?	You can specify either an external Symantec LiveUpdate server (recommended), or one or more internal LiveUpdate servers that have previously been installed and configured. You should not install Symantec Endpoint Protection Manager and an internal LiveUpdate server on the same physical hardware or virtual machine. Installation on the same computer can result in significant server performance problems. If you decide to use one or more internal LiveUpdate servers, you may want to add the Symantec public LiveUpdate server as the last entry. If your clients cannot reach any server on the list, then they are still able to update from the Symantec LiveUpdate server. To continue using an internal LiveUpdate server, you should upgrade to the latest version of LiveUpdate Administrator. See: • Downloading LiveUpdate Administrator • Configuring clients to download content from an external LiveUpdate server • Configuring clients to download content from an internal LiveUpdate server • Choose a distribution method to update content on clients
How many content revisions should the site store?	The management server stores only the most recent full content package, plus incremental deltas for as many revisions as you specify here. This approach reduces the disk space that is required to store multiple content revisions on the server. The number of clients you select during the Symantec Endpoint Protection Manager installation defines the number of revisions the server stores. For each LiveUpdate content type, the default values are as follows: • If you do not check Management server will manage fewer than 500 clients, Symantec Endpoint Protection Manager stores 21 revisions. • If you check Management server will manage fewer than 500 clients, Symantec Endpoint Protection Manager stores 90 revisions. In most instances during an upgrade, the installation increases the number of revisions to match these new defaults. This increase occurs if the number of revisions you had before the upgrade is less than the new minimum default, based on the above criteria. See: Reverting to an older version of the Symantec Endpoint Protection security updates
How often should my site check for LiveUpdate content updates?	The default schedule of having Symantec Endpoint Protection Manager run LiveUpdate every four hours is a best practice.
What operating systems am I downloading content to?	LiveUpdate only downloads the content for the specified operating systems.
What content types should I download to the site and to the clients?	Make sure that the site downloads all content updates that are specified in your client LiveUpdate Content policies. See: • About the types of content that LiveUpdate downloads • Reverting to an older version of the Symantec Endpoint Protection security updates
What languages should be downloaded for product updates?	This setting applies to product updates only; the content updates are downloaded automatically for all languages.

Decision	Description
What content size should be downloaded for definitions?	Standard and embedded/VDI clients use a reduced-size set of definitions (only the latest) that is cloud-enabled. Scans on these clients automatically use the extended definitions set in the cloud. The dark network client downloads the entire set of definitions. Warning! Your management server must download the correct content for the client types in your network. If the management server does not download the content that your installed clients require, the clients cannot get updates from the management server.
Should I test engine updates before they are released?	For large organizations, you should test the new engine updates and definitions before they are rolled out to all client computers. You want to test new engine updates with the minimal amount of disruption and downtime. See: Testing engine updates before they release on Windows clients

Downloading content from a LiveUpdate server to the Symantec Endpoint Protection Manager

When you download content to a management server, you download it for all the management servers within the site.

To configure a site to download content

1. In the console, click **Admin > Servers**.
2. Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.
3. On the **LiveUpdate** tab, make choices from the following available options.
4. Under **LiveUpdate Source Servers**, click **Edit Source Servers** and then inspect the current LiveUpdate server that is used to update the management server. This server is the Symantec LiveUpdate server by default. Then do one of the following:
 - To use the existing LiveUpdate Source server, click **OK**.
 - To use an internal LiveUpdate server, click **Use a specified internal LiveUpdate server** and then click **Add**.

If you selected **Use a specified internal LiveUpdate server**, in the **Add LiveUpdate Server** dialog box, complete the boxes with the information that identifies the LiveUpdate server, and then click **OK**.

You can add more than one server for failover purposes. If one server goes offline, the other server provides support. You can also add the Symantec public LiveUpdate server as the last server in the list. If you add the public server, use <http://liveupdate.symantecliveupdate.com> as the URL.

NOTE

If you use a UNC server, then LiveUpdate requires that you use the domain or workgroup as part of the user name.

If the computer is in a domain, use the format domain_name\user_name.

If the computer is in a workgroup, use the format computer_name\user_name.

In the **LiveUpdate Servers** dialog box, click **OK**.

5. Under **Disk Space Management for Downloads**, type the number of LiveUpdate content revisions to keep.
6. In the **Download Schedule** group box, click **Edit Schedule**, set the options for how often the server should check for updates. Click **OK**.
7. Under **Platforms to Download**, click **Change Platforms** and then inspect the platforms list. Uncheck the platforms that you do not want to download content to.
8. Under **Content Types to Download**, inspect the list of update types that are downloaded.
To add or delete an update type, click **Change Selection**, modify the list, and then click **OK**.
The list should match the list of content types that you include in the LiveUpdate Content policy for your client computers.
9. Under **Content to Download for Client Types**, decide whether to download and store content for standard and embedded/VDI clients or dark network clients.

WARNING

You must download content for the client types in your network. If you do not download the content that your installed clients require, the clients cannot get updates from the management server.

To modify the setting, click **Change Selection**, modify the selection, and then click **OK**.

10. Under **Languages to Download**, inspect the list of languages of the update types that are downloaded.

To add or delete a language, click **Change Selection**, modify the list, and then click **OK**.

11. Click **OK** to save your selections and close the window.

More information

[How to update content and definitions on the clients](#)

Checking that Symantec Endpoint Protection Manager has the latest content

LiveUpdate downloads definitions and other content to Symantec Endpoint Protection Manager on a schedule. However, you can download content at any time if Symantec Endpoint Protection Manager does not have the latest version. Symantec Endpoint Protection Manager then provides this content to the client computers through the default LiveUpdate policy.

To check that Symantec Endpoint Protection Manager has the latest content

1. In the console, click **Home**.
2. In the Endpoint Status group box, under **Windows Definitions**, compare the dates for **Latest on Manager** and **Latest from Symantec**.
3. If the dates do not match, click **Admin > Servers > Local Site (My Site)**.
4. Under **Tasks**, click **Download LiveUpdate content > Download**.

If you are unable to update content on Symantec Endpoint Protection Manager through LiveUpdate, you can download a .jdb file from Symantec Security Response. Symantec Endpoint Protection Manager processes the contents of these files and makes them available for clients to download. See:

[Download .jdb files to update definitions for Endpoint Protection Manager](#)

Checking when content was downloaded from LiveUpdate to Symantec Endpoint Protection Manager

You can determine the date and time when content was last updated on Symantec Endpoint Protection Manager from LiveUpdate.

To check which content was downloaded from LiveUpdate to Symantec Endpoint Protection Manager

1. In the console, click **Admin**.
2. On the **Admin** page, under **Tasks**, click **Servers** and select the site.
3. Do either one of the following tasks:
 - To check the status of the download, click **Show the LiveUpdate Status**.
 - To check the version of the current content that the Symantec Endpoint Protection Manager is using, click **Show the LiveUpdate Status**.
4. Click **Close**.

More information

- [Troubleshoot LiveUpdate and definition issues with Endpoint Protection Manager](#)
- [Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

About the types of content that LiveUpdate downloads

By default, Symantec Endpoint Protection Manager downloads all types of content from the public Symantec LiveUpdate servers. The LiveUpdate Content policy then downloads all types of content from Symantec Endpoint Protection Manager to the Windows and Mac clients.

If you do exclude a content type from the site but you remove the content in a LiveUpdate Content policy, that content is not delivered to the clients. Typically, you should not need to exclude the content that Symantec Endpoint Protection Manager downloads. Do not exclude a type of content unless you are certain that you do not need it.

See: [Reverting to an older version of the Symantec Endpoint Protection security updates](#)

LiveUpdate does not download updated policies. Symantec Endpoint Protection Manager updates policies to clients when you assign a new policy to a group or when you edit an existing policy.

Table 162: The content types that you can download from LiveUpdate to the Symantec Endpoint Protection Manager

Content type	Description
Client product updates	Includes software improvements and critical fixes against security vulnerabilities to the Windows client. For example, an attacker could bypass a Symantec Endpoint Protection protection feature. LiveUpdate downloads the product updates as a full client installation package between RUx releases. Each package carries the same version number but has an updated build number. For example, the first client installation package might be labeled as 14.3.4555.2000 and the second as 14.3.5228.1000. When this option is enabled, the most recent interim package appears in the following locations in the Version Selection drop-down list: • AutoUpgrade wizard: On the Admin page > Install Packages page > Client Install Package > Upgrade Clients with Package > Upgrade Settings option > General tab. The AutoUpgrade wizard displays the most recent build only. • New package: On the Clients page > Install Packages tab > Add a Client Install Package > General tab. This option does not upgrade client installation packages that are new releases and that have major features in them, such as 14.3 RU2 to 14.3 RU3. You must still upgrade using AutoUpgrade or by manually downloading and installing a full client installation package through the Broadcom Download Management page. To update your Mac and Linux clients, you must use the Web link and email and Save package options in the Client Deployment Wizard. In 14.3 RU1 MP1 and earlier, keep this setting unchecked as this option was not used. See: • Upgrading to a new release • Upgrading client software with AutoUpgrade
Client patches	Includes the same client software improvements and security fixes as product updates, but the patches are downloaded as an incremental delta file (.dax) instead of the full client installation package. To download the content to the clients, go to the LiveUpdate Settings policy > Additional Settings tab, and check Download client patches. This option lets you update client patches from LiveUpdate, the management server, or a Group Update Provider to the clients. This option was renamed from Client security patches in 14.3 RU2.
Virus and Spyware definitions	Separate virus definition packages are available for the x86 and the x64 platforms. This content type also includes the Auto-Protect portal list as well as Power Eraser definitions.
SONAR heuristic signatures	Protects against zero-day attack threats.
Intrusion Prevention signatures	Protects against network threats and host vulnerabilities. Supports the intrusion prevention and detection engines and Memory Exploit Mitigation.

Content type	Description
Host Integrity content	Includes the templates of predefined requirements that enforce updated patches and security measures on the client computer. LiveUpdate downloads templates for the computers that run Windows operating systems and Mac operating systems. See: Adding a custom requirement from a template
Submission Control signatures	Controls the flow of submissions to Symantec Security Response.
Reputation Settings	Includes the updates to the reputation data that is used in protection.
Extended File Attributes and Signatures	Used to make updating certificates and Download Insight more data-driven. These data-driven downloads help Symantec update trusted signature lists with definition-style updates.
Endpoint Detection and Response	Updates to the Endpoint Detection and Response (EDR) component, which detects and investigates suspicious activities and issues on hosts and endpoints. EDR provides this forensic information to various product components, including submissions and EDR servers. Added in version 14. See: Endpoint Detection and Response engine updates for 14 RU1 and newer clients
Common Network Transport Library and Configuration	Definitions that the entire product uses to achieve network transportation and telemetry. These definitions are necessary for reputation queries, as well as for submissions and communication with EDR. Definitions in this category include SEPM STIC and SEPC STIC, for the Symantec Endpoint Protection Manager and Symantec Endpoint Protection client, respectively.
Advanced Machine Learning	Definitions that are used in virus and spyware scans for the clients that use a low-bandwidth policy. Use low-bandwidth mode for standard clients and embedded clients in a network with a slow Internet connection. In low-bandwidth mode, LiveUpdate downloads the definitions once per week or less frequently. To use low-bandwidth mode, you must enroll in the cloud and enable the Low Bandwidth policy. Low-bandwidth mode does not work with dark network clients. If you do not enroll the management server in the cloud console, or you do not intend on using a low-bandwidth policy, disable this option to save some bandwidth and disk space on Symantec Endpoint Protection Manager. See: Updating clients in low-bandwidth environments
Web and Cloud Access Protection	Definitions that from Symantec Cloud Secure Web Gateway (Cloud SWG). Web and Cloud Access Protection uses Cloud SWG servers to provide secure proxy settings for your web browsers.
SymPlatform definitions (SEF)	Symantec Endpoint Foundation (SEF) is a framework that delivers future protection technologies as content through LiveUpdate. SEF enables you to download new features to your clients without needing to upgrade them. Includes definitions for URL reputation (14.3 RU1 or later) and Auto-Protect (14.3 RU3 or later).
Application Control content	Definitions that the Application Control engine uses for the Application Control policy. You should always keep this option enabled. This content runs on version 14.2 and later clients only. For older Windows clients, you must upgrade them to 14.2 first.
Policy Command Handler	Content used by the Policy Command Handler engine.
Endpoint Threat Defense for AD Data	Content used by the Active Directory Defense engine. Added in 14.2 RU1.
Browser Extension	Content for the IPS engine that the client uses to block malicious websites on Google Chrome. Added in 14.3 RU2.
Attack Surface Reduction	The integration component for Application Hardening for hybrid-managed clients. Includes Application Control, Adaptive Isolation, and Application Discovery. Added in 14.3 RU5.

For more information, see:

[LiveUpdate Administrator content options for Endpoint Protection 14](#)

You cannot disable the following types of content in the LiveUpdate Content policy, including **Extended File Attributes and Signatures**, **Endpoint Detection and Response**, **Common Network Transport Library and Configuration**.

Table 163: Features and the update content that they need

When you install an unmanaged client	When you update, you need to download these types of content
Virus and Spyware Protection	• Virus and Spyware Definitions • SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. • Centralized Reputation Settings When you configure content types for download in Site Properties, this content type is called Reputation Settings. • Revocation Data (downloaded by default, not configurable from Symantec Endpoint Protection Manager) • Symantec Allow List (Symantec Whitelist) • Submission Control signatures • Auto-Protect portal list • Power Eraser definitions • Extended File Attributes and Signatures • Endpoint Detection and Response • Common Network Transport Library and Configuration • Advanced Machine Learning
Virus and Spyware Protection > Download Protection	• Virus and Spyware Definitions • SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. • Centralized Reputation Settings • Revocation Data • Symantec Allow List (Symantec Whitelist) • Intrusion Prevention signatures When you select this option to download, it includes updates to both the Intrusion Prevention signatures and the Intrusion Prevention engines. • Submission Control signatures • Auto-Protect portal list • Power Eraser definitions • Extended File Attributes and Signatures • Endpoint Detection and Response • Common Network Transport Library and Configuration • Advanced Machine Learning

When you install an unmanaged client	When you update, you need to download these types of content
Virus and Spyware Protection > Outlook Scanner	• Virus and Spyware Definitions • SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. • Centralized Reputation Settings • Revocation Data • Symantec Allow List (Symantec Whitelist) • Submission Control signatures • Auto-Protect Portal List • Power Eraser Definitions • Extended File Attributes and Signatures • Endpoint Detection and Response • Common Network Transport Library and Configuration • Advanced Machine Learning
Virus and Spyware Protection > Notes Scanner	• Virus and Spyware Definitions • SONAR Definitions When you configure content types for download in Site Properties, these are called SONAR heuristic signatures. • Centralized Reputation Settings • Revocation Data • Symantec Allow List (Symantec Whitelist) • Submission Control signatures • Auto-Protect Portal List • Power Eraser Definitions • Extended File Attributes and Signatures • Endpoint Detection and Response • Common Network Transport Library and Configuration • Advanced Machine Learning
Proactive Threat Protection > SONAR	SONAR Definitions Submission Control signatures Extended File Attributes and Signatures Advanced Machine Learning
Proactive Threat Protection > Application Control	Submission Control signatures Extended File Attributes and Signatures Application Control content
Web and Cloud Access Protection policy	Web and Cloud Access Protection
Network and Host Exploit Mitigation > Intrusion Prevention	• Intrusion Prevention signatures When you select this option to download, it includes updates to both the intrusion prevention signatures and the Intrusion Prevention engines. • Submission Control signatures • Extended File Attributes and Signatures • Browser Extension (as of 14.3 RU2)
Network and Host Exploit Mitigation > Firewall	Submission Control signatures Extended File Attributes and Signatures
Host Integrity	Host Integrity content Submission Control signatures Extended File Attributes and Signatures

More information

- [Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)
- [How to update content and definitions on the clients](#)
- [Choose a distribution method to update content on clients](#)

Configuring clients to download content from an internal LiveUpdate server

By default, your Windows clients get their updates from the management server.

NOTE

For Mac and Linux clients, you either need to configure the management server to act as a reverse proxy, or you need to use LiveUpdate Administrator.

[Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy](#)

If you manage a large number of clients, you may want to use Group Update Providers (GUPs) for Windows clients. GUPs reduce the load on the management server and are easier to set up than an internal LiveUpdate server. See:

[Using Group Update Providers to distribute content to clients](#)

If you don't want to use the default management server or Group Update Providers for client updates, you can:

- Set up an internal LiveUpdate server.
- Use a Symantec LiveUpdate server that is external to your network.

To use an internal LiveUpdate server, you must perform the following tasks:

- Install the internal LiveUpdate server.

For more information about using an internal LiveUpdate server, refer to the *LiveUpdate Administrator's Guide*.

NOTE

Symantec Endpoint Protection Manager no longer includes legacy support for LiveUpdate Administrator 1.x. To continue using an internal LiveUpdate server, you should upgrade to the latest version of LiveUpdate Administrator. Support for LiveUpdate Administrator 2.x and later is always enabled.

- Use the LiveUpdate Settings policy to configure your clients to use that internal LiveUpdate server.

NOTE

You can specify proxy settings for the clients that connect to an internal LiveUpdate server for updates. The proxy settings are for updates only. They do not apply to other types of external communication that clients use. You configure the proxy for other types of client external communication separately. See:

[Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server](#)

To configure Windows clients to use an internal LiveUpdate server:

1. Under **Policies**, click **LiveUpdate**.
2. On the **LiveUpdate Settings** tab, open the policy that you want to edit.
3. Under **Windows Settings**, click **Server Settings**.
4. In the **Server Settings** pane, check **Use a LiveUpdate server**.
5. Click **Use a specified internal LiveUpdate server**, and then click **Add**.
6. In the **Add LiveUpdate Server** dialog box, type the information that you need to identify and communicate with the server that you want to use.

For the **URL**:

-
- You can use the HTTP or the HTTPS method. Type the URL for the server. For example: Domain name: `http://myliveupdateserver.com`
 - IPv4 address: `http://192.168.133.11:7070/clu-prod`
 - IPv6 address: `http://[fd00:fe32::b008]:7070/clu-prod`

NOTE

Support for the FTP method or the UNC method was removed in 14.3 RU1. In earlier versions:

- If you use the FTP method, type the FTP address for the server. For example: `ftp://myliveupdateserver.com`
- If you use the LAN method, type the server UNC path name. For example: `\\myliveupdateserver\\LUDepot`

7. If required, type in a user name and password for the server, and then click **OK**.

NOTE

If you use a UNC server, then LiveUpdate requires that you use the domain or workgroup in addition to the user name. If the computer is part of a domain, use the format `domain_name\user_name`. If the computer is part of a workgroup, use the format `computer_name\user_name`.

8. Under **LiveUpdate Policy**, click **Schedule** to set up a schedule for updates through LiveUpdate, and then click **OK**. See:

[Configuring the LiveUpdate download schedule to client computers](#)

9. Optionally click **Advanced Settings**.

Decide whether to keep or change the default user settings, product update settings, and non-standard header settings. Generally, you do not want users to modify update settings. You may, however, want to let users manually launch a LiveUpdate session if you do not support hundreds or thousands of clients. See:

[Configuring the amount of control that users have over LiveUpdate](#)

10. Click **OK**.

To configure Mac clients or Linux clients to use an internal LiveUpdate server:

1. On the **Policies** page, click **LiveUpdate**.
2. On the **LiveUpdate Settings** tab, open the policy.
3. Under **Mac Settings** or **Linux Settings**, click **Server Settings**.
4. Click **Use a specified internal LiveUpdate server**, and then click **Add**.
5. In the **Add LiveUpdate Server** dialog box, type the information that you need to identify and communicate with the server that you want to use.

For the **URL**:

- You can use the HTTP or the HTTPS method. Type the URL for the server. For example: Domain name: `http://myliveupdateserver.com`
 - IPv4 address: `http://192.168.133.11:7070/clu-prod`
 - IPv6 address: `http://[fd00:fe32::b008]:7070/clu-prod`

NOTE

Support for the FTP method or the UNC method was removed in 14.3 RU1.

6. If required, type in a user name and password for the server and then click **OK**.
7. If your server uses FTP, click **Advanced Server Settings**, click the FTP mode that the server uses, either **Active** or **Passive**, and then click **OK**.
8. To modify the schedule, click **Schedule**.
9. Click **OK**.

More information

- [Randomizing content downloads from a LiveUpdate server](#)
- [Configuring Windows client updates to run when client computers are idle](#)
- [Choose a distribution method to update content on clients](#)

Configuring clients to download content from an external LiveUpdate server

By default, Symantec Endpoint Protection Manager provides updates to Windows clients. To help mitigate network overloads for Windows client updates, you should also let clients get updates from a LiveUpdate server. Linux and Mac clients must get updates from a LiveUpdate server, or you can set up the Apache web server as a reverse proxy to download updates from the management server. See:

- [Choose a distribution method to update content on clients](#)
- [Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy](#)

NOTE

You may also want to establish communication between a proxy server and Symantec Endpoint Protection Manager so that it can connect with Symantec subscription services. A proxy server can provide an additional level of protection between your site and an external Symantec LiveUpdate server. See:

[Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate](#)

To configure clients to download content from an external LiveUpdate server

1. In the console, open a LiveUpdate policy, and click **Edit**
2. Under **Windows Settings**, **Mac Settings**, or **Linux Settings**, click **Server Settings**.
3. Click **Use the default Symantec LiveUpdate server** or specify another LiveUpdate server. If needed, specify your proxy configuration.
4. Click **OK**.

More information

[How to update content and definitions on the clients](#)

Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

You can configure Symantec Endpoint Protection Manager to go through a proxy server to connect to the Internet. A proxy server can add a layer of security because only the proxy server is connected directly to the Internet.

To configure Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, select the management server to which you want to connect a proxy server.
3. Under **Tasks**, click **Edit the server properties**.
4. On the **Proxy Server** tab, under either **HTTP Proxy Settings** or **FTP Proxy Settings**, for **Proxy usage**, select **Use custom proxy settings**.
5. Type in the proxy settings.
For more information on these settings, click **Help**.
6. Click **OK**.

More information

[Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server](#)

Specifying a proxy server that clients use to communicate to Symantec LiveUpdate or an internal LiveUpdate server

You can specify a proxy server that your clients use to communicate with an internal LiveUpdate server. The proxy settings do not affect any settings for Group Update Providers.

NOTE

You configure proxy settings for other client communications separately.

To specify a proxy server that clients on Windows computers or Linux computers use to communicate to Symantec LiveUpdate or an internal LiveUpdate server

1. In the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**, and then click the **LiveUpdate Settings** tab.
3. Right-click the policy that you want and then select **Edit**.
4. Under **Windows Settings** or under **Linux Settings**, click **Server Settings**.
5. Under **LiveUpdate Proxy Configuration**, click **Configure Proxy Options**.
6. Do one of the following:
 - For Windows clients, on the **HTTP or HTTPS** tab, select the desired options. You can also specify proxy settings for FTP.
 - For Linux clients, on the **HTTP** tab, select the desired options.See the online Help for more information about the options.
7. Click **OK** in the dialog box.
8. Click **OK**.

To specify a proxy server that clients on Mac computers use to communicate to Symantec LiveUpdate or an internal LiveUpdate server

1. In the console, click **Clients > Policies**.
2. Under **Location-independent Policies and Settings**, under **Settings**, click **External Communication Settings**.
3. On the **Proxy Server (Mac)** tab, select the desired options.
4. Click **OK**.

More information

[How to update content and definitions on the clients](#)

Configuring the LiveUpdate download schedule to client computers

The LiveUpdate client schedule settings are defined in the LiveUpdate Settings policy. These settings apply to LiveUpdate sessions that get the latest updates from either a Symantec LiveUpdate server or an internal LiveUpdate server. See:

- [Configuring clients to download content from an external LiveUpdate server](#)
- [Configuring clients to download content from an internal LiveUpdate server](#)

To save bandwidth, you can let your clients run scheduled LiveUpdate sessions only if either of the following conditions is met:

- Virus and spyware definitions on a client computer are more than 2 days old.
- A client computer is disconnected from Symantec Endpoint Protection Manager for more than 8 hours.

NOTE

To make sure that any client computers that connect to your network infrequently get the latest updates, let these computers get updates from a Symantec LiveUpdate server. These servers are public, and the client therefore does not depend on a connection to your network to get updates.

To configure the schedule for LiveUpdate downloads to Windows client computers

1. Click **Policies** and then click **LiveUpdate**.
2. On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.
3. Under **Windows Settings**, click **Schedule**.
4. Make sure that **Enable LiveUpdate Scheduling** is checked. This option is enabled by default.

NOTE

You should not uncheck this box. If you disable **LiveUpdate Scheduling**, clients do not get the latest updates.

5. Specify the frequency.
If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.
6. If you select any frequency other than **Continuously**, specify the **Retry Window**.
The **Retry Window** is the number of hours or days that the client computer tries to run LiveUpdate if the scheduled LiveUpdate fails for some reason.
7. Set any additional options, if required. Symantec recommends that you keep the default values for running LiveUpdate if the definitions are out of date, or if the client has not connected recently to the management server.
8. Click **OK**.

[Randomizing content downloads from a LiveUpdate server](#)

To configure the schedule for LiveUpdate downloads to Mac client computers

1. Click **Policies** and then click **LiveUpdate**.
2. On the **LiveUpdate Settings Policy** tab, right-click the policy that you want, and then click **Edit**.
3. Under **Mac Settings**, click **Schedule**.
4. Specify the frequency.
If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.
5. Click **OK** when finished.

To configure the schedule for LiveUpdate downloads to Linux client computers

1. On the **LiveUpdate Settings Policy** tab, right-click the policy that you want, and then click **Edit**.
2. Under **Linux Settings**, click **Schedule**.
3. Specify the frequency.
If you select **Daily**, also set the time of day to run. If you select **Weekly**, also set the time of day to run and the day of the week to run.
You can also randomize content downloads.
4. Click **OK**.

More information

[How to update content and definitions on the clients](#)

Configuring the amount of control that users have over LiveUpdate

You may want to allow users who travel to use an Internet connection to get updates directly from a Symantec LiveUpdate server. You can also allow users to modify the LiveUpdate schedule you set up for content downloads.

NOTE

If an unmanaged client has a LiveUpdate Settings policy assigned to it when an install package is created, the SEPM policy settings always take precedence over a user's changes. To install an unmanaged client so that a user's changes takes precedence, install the client from the installation file.

To configure the amount of control that users have over LiveUpdate

1. In the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want, and then click **Edit**.
4. Under **Windows Settings**, click **Advanced Settings**.
5. Under **User Settings** pane, check **Allow the user to manually launch LiveUpdate**.
6. Optionally, check **Allow the user to modify the LiveUpdate schedule**.
7. Click **OK**.

More information

- [Reverting to an older version of the Symantec Endpoint Protection security updates](#)
- [Configuring the LiveUpdate download schedule to client computers](#)

Mitigating network overloads for client update requests

You must manage your networks for the critical but infrequent situation when too many clients simultaneously request a full set of virus and spyware definitions from the management server or from a Group Update Provider. This situation can occur if the management server encounters an error or runs out of disk space, so that the download and update of the definitions on the client then fails. This situation can also occur if the management server does not download a definitions package and a client then requests this specific delta. In either case, the client then must request a package with a full set of definitions from either the management server or from the Group Update Provider.

To help prevent overloads on your network, the management server provides the following features:

- A notification when the management server receives a specified number of requests for a full set of definitions within a specified period of time.
You set the conditions for this notification based on what constitutes an overload for your environment. To configure the notification, add a **Network load: requests for virus and spyware full definitions** notification condition. See: [Setting up administrator notifications](#)
- The ability to let clients get deltas for virus and spyware definitions from a LiveUpdate server if the management server can provide only a full set. In a LiveUpdate Settings policy, click **Advanced Settings > Download delta content from a LiveUpdate server when available**.
This option was renamed from **Download smaller client installation packages from a LiveUpdate server when available** in 14.3 RU2.
- The ability to block clients from downloading a full set of virus and spyware definitions from the management server. If you receive a notification of a network overload, you can block any further downloads of full packages from the management server. You cannot, however, stop any downloads that are already in progress. Configure this option by clicking **Admin > Servers > server_name > Edit the server properties > Full Definitions Download > Prevent clients from downloading full definition packages**. See: [Full Definitions Download](#)

About randomization of simultaneous content downloads

The Symantec Endpoint Protection Manager supports randomization of simultaneous content downloads to your clients from the default management server or a Group Update Provider. It also supports the randomization of the content downloads from a LiveUpdate server to your clients. Randomization reduces peak network traffic and is on by default.

You can enable or disable the randomization function. The default setting is enabled. You can also configure a randomization window. The management server uses the randomization window to stagger the timing of the content downloads. Typically, you should not need to change the default randomization settings.

In some cases, however, you might want to increase the randomization window value. For example, you might run the Symantec Endpoint Protection client on multiple virtual machines on the same physical computer that runs the management server. The higher randomization value improves the performance of the server but delays content updates to the virtual machines.

You also might want to increase the randomization window when you have many physical client computers that connect to a single server that runs the management server. In general, the higher the client-to-server ratio, the higher you might want to set the randomization window. The higher randomization value decreases the peak load on the server but delays content updates to the client computers.

In a scenario where you have very few clients and want rapid content delivery, you can set the randomization window to a lower value. The lower randomization value increases the peak load on the server but provides faster content delivery to the clients.

For downloads from the default management server or a Group Update Provider, you configure the randomization settings in the **Communication Settings** dialog box for the selected group. The settings are not part of the LiveUpdate Settings policy.

For downloads from a LiveUpdate server to your clients, you configure the randomization setting as part of the LiveUpdate Settings policy.

More information

- [Randomizing content downloads from the default management server or a Group Update Provider](#)
- [Randomizing content downloads from a LiveUpdate server](#)
- [Configuring clients to download content from an internal LiveUpdate server](#)

Randomizing content downloads from the default management server or a Group Update Provider

Your default management server or Group Update Providers might experience reduced performance when multiple client computers attempt to download content from them simultaneously. You can set a randomization window in the communication settings for the group to which the client computers belong. Each client computer attempts to download content at a random time that occurs within that window.

NOTE

The communication settings do not control the randomization settings for the client computers that download content from a LiveUpdate server. You can change the randomization settings for those computers in the LiveUpdate Settings policy. See:

[Randomizing content downloads from a LiveUpdate server](#)

To randomize content downloads from the default management server or a Group Update Provider

-
1. In the console, click **Clients**.
 2. Under **Clients**, click the group that you want.
 3. On the **Policies** tab, under **Location-independent Policies and Settings**, under **Settings**, click **Communication Settings**.
 4. In the **Communication Settings** dialog box, under **Download Randomization**, check **Enable randomization**.
 5. Optionally, change the randomization window duration.
 6. Click **OK**.

More information

- [About randomization of simultaneous content downloads](#)
- [Configuring clients to download content from an internal LiveUpdate server](#)

Reducing network congestion due to synchronous SEP client LiveUpdate content downloads

Randomize the timing of SEP Windows and Linux clients LiveUpdate content downloads to free-up network resources.

LiveUpdate content downloads can be taxing on your network when multiple SEP Windows and Linux clients perform downloads simultaneously. Reduce the strain on your network by configuring client computers to schedule LiveUpdate content downloads at random times. Randomizing client content downloads ensures that clients perform LiveUpdate content downloads at varying times, which can free up network resources.

NOTE

The LiveUpdate policy schedule settings do not control randomization for the client computers that download content from the default management server or from a Group Update provider. You can change the randomization settings for those computers in the **Communication Settings** dialog box for the group to which they belong. See:

[Randomizing content downloads from the default management server or a Group Update Provider](#)

To randomize content downloads from a LiveUpdate server

1. Click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.
4. Under **Windows Settings**, **Mac Settings**, or **Linux Settings**, click **Schedule**.
5. Under **Download Randomization Options**, check **Randomize the start time to be + or - (in hours)**.

NOTE

This setting is in days, if you select **Weekly** updates.

6. Optionally, change the duration for the randomized start time.
7. Click **OK**.

More information

- [About randomization of simultaneous content downloads](#)
- [Configuring clients to download content from an internal LiveUpdate server](#)

Configuring Windows client updates to run when client computers are idle

To ease Windows client computer performance issues, you can configure content downloads to run when client computers are idle. This setting is on by default. Several criteria, such as user, CPU, and disc actions, are used to determine when the computer is idle.

If **Idle Detection** is enabled, once an update is due, the following conditions can delay the session:

- The user is not idle.
- The computer is on battery power.
- The CPU is busy.
- The disk I/O is busy.
- No network connection is present.

After one hour, the blocking set is reduced to CPU busy, Disk I/O busy, or no network connection exists. Once the scheduled update is overdue for two hours, as long as a network connection exists, the scheduled LiveUpdate runs regardless of idle status.

To configure Windows client updates to run when client computers are idle

1. Click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.
4. Under **Windows Settings**, click **Schedule**.
5. Check **Delay scheduled LiveUpdate until the computer is idle. Overdue sessions will run unconditionally**.
6. Click **OK**.

More information

- [Configuring the LiveUpdate download schedule to client computers](#)
- [Configuring Windows client updates to run when definitions are old or the computer has been disconnected](#)

Configuring Windows client updates to run when definitions are old or the computer has been disconnected

You can ensure that Windows clients update when definitions are old, or the computer has been disconnected from the network for a specified amount of time.

NOTE

If you check both available options, the client computer must meet both conditions.

To configure Windows client updates when definitions are old or the computers is disconnected from the manager

-
1. Click **Policies**.
 2. Under **Policies**, click **LiveUpdate**.
 3. On the **LiveUpdate Settings** tab, right-click the policy that you want to edit, and then click **Edit**.
 4. Under **Windows Settings**, click **Schedule**.
 5. Check **LiveUpdate runs only if Virus and Spyware definitions are older than:** and then set the number of hours or days.
 6. Check **LiveUpdate runs only if the client is disconnected from Symantec Endpoint Protection Manager for more than:** and then set the number of minutes or hours.
 7. Click **OK**.

More information

- [Configuring the LiveUpdate download schedule to client computers](#)
- [Configuring Windows client updates to run when client computers are idle](#)

Configuring clients to download content from the Symantec Endpoint Protection Manager

The default method for downloading content to clients is by using the management server.

You do not define the schedule for the updates from the management server to the clients. The clients download content from the management server based on the communication mode and heartbeat frequency.

To configure clients to download content from the Symantec Endpoint Protection Manager

1. In the console, open a LiveUpdate policy, and click **Edit**
2. Under **Windows Settings**, click **Server Settings**.
3. Make sure that **Use the default management server** is checked.
4. Click **OK**.

More information

[Updating policies and content on the client using push mode or pull mode](#)

Testing engine updates before they release on Windows clients

Symantec Endpoint Protection contains several engines that carry out parts of its functionality. These engines are binary files (.dll or .exe) and are delivered with the security definitions. Symantec updates the functionality of these engines to enhance Symantec Endpoint Protection's capabilities and to respond to new threats.

While Symantec updates virus definitions several times a day, the engine content is updated on a quarterly basis. Symantec provides the engine updates using LiveUpdate.

Symantec provides a special server lets you download and test the engine content before you roll out the content to your production environment. Symantec releases these updates on the Early Adopter server (EAS). Engine updates are released a few weeks before the engines are available for general release on the public LiveUpdate server.

You download the engine updates using the EAS, try them in a lab environment, and let Symantec know of any conflicts you encounter. This process lets Symantec fix these conflicts ahead of the general release.

Use the following process to test engine updates.

-
- [Step 1: Create a group of test computers to receive content](#)
 - [Step 2: Configure test computers to receive prereleased content from the Early Adopter server](#)
 - [Step 3: Configure test and non-test computers to a particular engine version](#)
 - [Step 4: Set up notifications for new engine releases \(optional\)](#)
 - [Step 5: Monitor the test computers after engine content is released](#)

Step 1: Create a group of test computers to receive content

The most accurate test of engine compatibility is with the production systems that do real work. Create a permanent testing group by selecting a set of client computers to receive EAS content using the following criteria:

- Identify the various types of critical systems within your environment. These systems may vary from each other by hardware, software, or function. For example, you might identify retail systems such as a gold desktop image, point-of-sale systems, and web servers, among other critical systems to test.
- Use multiple systems of each type as some software conflicts may manifest only intermittently. Choose the production systems that already have the installed software that you normally use and that perform a representative load of work.
- Configure the test client computers that receive the early release content like the production computers that you do not test. Both the clients that you test and do not test should have the same Symantec Endpoint Protection features installed and use the same policies.

If you prefer not to use production computers for testing with the EAS, you may use lab-based systems. In this case, you may want to write the automation that exercises the functions of the systems under test and simulate load.

For customers with a small number of client computers, all you need is one Symantec Endpoint Protection Manager and one Symantec Endpoint Protection for Windows client.

Step 2: Configure test computers to receive prereleased content from the Early Adopter server

For the test group, configure LiveUpdate to download the content from the Symantec Early Adopter server by performing the following steps.

To configure a site to download content from the Symantec Early Adopter LiveUpdate server

1. In the console, click **Admin > Servers**.
2. Under **Servers**, right-click **Local Site**, and then click **Edit Site Properties**.
3. Under **LiveUpdate Source Servers**, click **Edit Source Servers**.
4. In the **LiveUpdate Servers** dialog box, click **Use the Symantec LiveUpdate server for prereleased content**, and then click **OK > OK**.

To configure the managed clients to use the prerelease Symantec Early Adopter LiveUpdate server

1. In the console, open a new LiveUpdate Settings policy, and click **Policies > LiveUpdate**.
2. Under **Windows Settings**, click **Server Settings > Use a LiveUpdate server > Use the Symantec LiveUpdate server for prereleased content**.
3. Click **OK**, and assign the policy to the test group.

As long as your LiveUpdate Settings policy gets content from the EAS, the test clients continue to receive the prereleased versions of the content.

NOTE

For non-test groups, keep the LiveUpdate Settings policy configured to the LiveUpdate server that you normally use. After the engines are available for general release, all client computers receive LiveUpdate content, depending on how you configured your client computers to receive it.

For more information, see:

-
- [Configuring clients to download content from an internal LiveUpdate server](#)
 - [Configuring clients to download content from an external LiveUpdate server](#)

Step 3: Configure test and non-test computers to a particular engine version

Configure several LiveUpdate Content policies so that:

- The test group receives the latest version of the security definitions and engines. This group downloads all future content revisions with the prerelease engine version in it.
- The non-test groups receive an existing, safe version of the engine.
You can also lock on an engine version. With this option, clients continue to receive the latest security definitions that are associated with a particular engine, but not the latest engine version. See:
[Reverting to an older version of the Symantec Endpoint Protection security updates](#)
After you are satisfied that the test group functions normally with the prereleased content, you manually choose the next engine version for these non-test groups.

Step 4: Set up notifications for new engine releases (optional)

To get notifications for planned engine releases that LiveUpdate downloads to the Symantec Endpoint Protection Manager, do one of the following tasks:

- Add a notification for when new content has been downloaded to Symantec Endpoint Protection Manager. Notifications for new content include new engine releases as well as security definitions. You receive notifications only if one or more LiveUpdate Content policies that specify a content revision by engine version are locked due to an available engine update.

To view notifications, on the **Home** page, in the **Security Status** pane, click **View Notifications**.

NOTE

Updates on the EAS are as frequent as on the regular LiveUpdate server. If you feel that you receive these notifications too often, configure the notifications to not appear.

For more information, see:

[Setting up administrator notifications](#)

- Premium Support Customers can log on here to the Customer Subscription Portal. See:
[How Premium Support Customers can sign up for alerts and notifications](#)

Step 5: Monitor the test computers after engine content is released

After Symantec publishes an engine update to the EAS, begin monitoring the computers that you configured to receive this content. Monitor the following items:

- Verify that the test computers run the prerelease version of the engine updates. See:
[Verifying which engine and definitions run on the client computers](#)
- Uptime and available resources on the servers and other critical infrastructure using tools such as Microsoft System Center Operations Manager.
- The applications that run on the client computers to ensure that they continue to perform as expected.
- The Symantec Endpoint Protection client status to ensure that it remains connected to the management server and is protected. See:
[Checking whether the client is connected to the management server and is protected](#)

In addition, run the client after you modify the policies or run a scan to ensure that the computer functions as expected.

If you notice any unexpected behavior or suspect a software conflict exists with the engine update, contact Support for assistance. Usually, if Symantec confirms that there is a software conflict before the beginning of the phased rollout, Symantec reschedules the publishing, and works with you to correct the issue. Symantec then republishes an updated engine to EAS.

Verifying which engine and definitions run on the client computers

In the management server and in the client, find the version numbers of the engines and the definitions that the client runs. Compare the date and revision number of the content that contains the updated engine. You can quickly determine which clients have the new engine and which clients still need the update.

To verify which engine version the clients run

1. In the Symantec Endpoint Protection Manager console, click the **Reports > Quick Reports** tab.
2. For the **report type**, select **Computer Status** and for **Select a report**, click **Client Inventory Details**.
3. Select a time range, click **Save Filter** to specify a report name, and then click **Create Report**.

The report shows the definitions dates and the revision numbers for all major content types. You can export this report to a .CSV file if needed.

Reporting - Client Inventory Details

Symantec Endpoint Protection

Client Inventory Details

Updated since 09/27/2016 12:47:00 [Print](#) [Save](#) [Close](#)

Description: This report contains details of client inventory.

Client Inventory Details

Computer Name	Health	Client Version	Virus Definitions	SONAR Definitions	IPS Signatures	Download Protection Content
	Offline	14.0.3263.1000	6/29/17 r4	6/26/17 r1	6/28/17 r21	6/28/17 r3

4. On the client, click **Help > Troubleshooting > Versions**.

You can also use the following method to confirm that the AV engine and Eraser engine updates have been successfully applied to the client. See:

- [How to check the version of AV Engine, IPS Engine and Eraser Engine from the client computer](#)
- [About Computer Status reports and logs](#)

What are the engines that Symantec Endpoint Protection runs?

The Security Response team maintains and updates the Endpoint Protection engine releases.

Symantec Endpoint Protection uses the following engine components on the Windows clients:

- **AntiVirus engine (AVE)** (Virus and Spyware Protection)
This unique scanning engine provides advanced file-based detection against the latest threats. A new release of the antivirus engine might change the amount of paged pool memory that Symantec Endpoint Protection uses. The files that the engine uses are signed by Symantec.
- **BASH engine** (SONAR)

Behavioral engine for SONAR which uses heuristics as well as file reputation data to make decisions about applications or files.

- **CIDS (Client Intrusion Detection System) engine** (Intrusion Prevention System, Memory Exploit Mitigation)
The CIDS engine works with the IPS definitions that protect against network attacks and browser attacks. For Browser Intrusion Prevention, support is based on the version of the CIDS engine that the client uses. Memory Exploit Mitigation (as of version 14) techniques also use the CIDS engine. See:
[Supported browsers for Browser Intrusion Prevention in Endpoint Protection](#)
- **Eraser engine** (Virus and Spyware Protection)
The Eraser engine is used to provide repair and removal capability (remediation) for the threats that are found on a customer's system. Eraser also checks that the drivers and applications that run at startup are not malicious. See:
[All About Eraser Updates and Application Testing After An Eraser Engine Update Is Applied](#)
- **Static Data Scanner (SDS) engine**
This engine and their definitions support the emulator, the Intelligent Threat Cloud Service (ITCS), and the CoreDef-3 definitions engine for advanced machine learning (AML) (as of version 14). The SDS engine determines whether a given boot sector, partition table, file, or process memory contains a threat. It repairs threats in certain conditions.

Reverting to an older version of the Symantec Endpoint Protection security updates

By default, the latest version of content that is downloaded from a LiveUpdate server to the management server is automatically downloaded to Windows clients. The LiveUpdate Content policy specifies the type of content that clients are permitted to check for and install.

However, you may need to download an older version of the content in the following cases:

- The latest set of definitions or engine causes a software conflict on the client computers.
- You want time to test new engines on control groups before the content releases into production.

NOTE

Use this feature very carefully. Unchecking a content type means that the feature is not kept up-to-date on the client. This can potentially put your clients at greater risk.

If you set the content type to **Select a revision** and then convert the Symantec Endpoint Protection client to a cloud-managed client, the content does not update on the client. To avoid this issue, make sure you set the content option to **Use latest available** before you convert the client.

To revert to an older version of the Symantec Endpoint Protection security updates

1. In the console, click **Policies > LiveUpdate**, and open a LiveUpdate Content policy.
2. Under **Windows Settings**, click **Security Definitions**.

You cannot roll back content for Mac clients or Linux clients.

3. To roll back the content to a specific version, click one of the following options:
 - **Select a revision > Edit**, and select the revision number.
This option locks the clients to one particular set of security definitions. The clients do not receive any new security definitions.
 - **Select an engine version > Edit**, and then select the engine version.
This option locks the clients to one particular engine, but continues to distribute the latest security definitions that are associated with that engine. Select the engine version if you know the current engine works in your environment, and you need to test a newer engine in a different group before you release it. Or, click **Use latest available** for clients to continually receive the latest engine version and definitions for that content type.

4. Click **OK**.

You do not need to restart the client computer for the content to update.

5. After you resolved any troubleshooting issues, under **Windows Settings**, click **Security Definitions > Use latest available** for each content type.

More information

- [Testing engine updates before they release on Windows clients](#)
- [Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

Using Group Update Providers to distribute content to clients

A Group Update Provider (GUP) is a client computer that distributes content updates directly to other clients.

Advantages of the GUPs include:

- They conserve bandwidth and management server resources by offloading processing power to the GUP.
- They deliver updates effectively to clients with limited or slow network connectivity.
- They are easier to set up than an internal LiveUpdate server.

Table 164: Tasks to use Group Update Providers

Step	Description
Step 1: Understand the differences between the types of Group Update Providers that you can configure	You can set up single, multiple, or cross-subnet Group Update Providers. The type of Group Update Provider that you set up depends on your network and the clients on that network. The types of Group Update Provider are not mutually exclusive. You can configure one or more types of Group Update Provider per policy. See: • About the types of Group Update Providers • About the effects of configuring more than one type of Group Update Provider in your network
Step 2: Verify client communication	Before you configure Group Update Providers, verify that the client computers can receive content updates from the server. Resolve any client-server communication problems. You can view client-server activity in the System logs on the Logs tab of the Monitors page. See: Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client
Step 3: Configure Group Update Providers in one or more LiveUpdate Settings policies	You configure Group Update Providers in the LiveUpdate Settings policy. See: Configuring clients to download content from Group Update Providers
Step 4: Assign the LiveUpdate Settings policy to groups	You assign the LiveUpdate Settings policy to the groups that use the Group Update Providers. You also assign the policy to the group in which the Group Update Provider resides. For a single Group Update Provider, you assign one LiveUpdate Settings policy per group per site. For multiple Group Update Providers and explicit lists of Group Update Providers, you assign one LiveUpdate Settings policy to multiple groups across subnets. See: Assigning a policy to a group or location
Step 5: Verify that clients are designated as Group Update Providers	To view the client computers that are designated as Group Update Providers, do one of the following tasks: • Click Clients > Clients tab > right-click the client, and then click Edit Properties. The Group Update Provider field is True or False. • Search for the clients that act as Group Update Providers. See: Searching for the clients that act as Group Update Providers

About the types of Group Update Providers

You can configure several types of Group Update Providers in a LiveUpdate Settings policy. The types of Group Update Providers that you use depend on how your network is set up. You can configure one or more types of Group Update Provider per policy; they are not mutually exclusive.

Table 165: When to use a particular type of Group Update Provider

Group Update Provider Type	When to use
Single	A single Group Update Provider is a dedicated client computer that provides content for one or more groups of clients. Configuring a single Group Update Provider turns a single client into a Group Update Provider. A single Group Update Provider can be a client computer in any group. Use a single Group Update Provider when you want to use the same Group Update Provider for all your client computers. You use a single LiveUpdate Settings policy to specify a static IP address or host name for a single Group Update Provider. However, if the client that serves as a single Group Update Provider changes location, you must change the IP address in the policy. If you want to use different single Group Update Providers in different groups, you must create a separate LiveUpdate Settings policy for each group.
Multiple	Multiple Group Update Providers use a set of rules, or criteria, to elect themselves to serve groups of clients in their own subnets. All client computers are on the same subnet. You specify the criteria that client computers must meet to qualify as a Group Update Provider. If a client computer meets the criteria, the management server adds the client to a global list of Group Update Providers. The management server then makes the global list available to all the clients in the network. Clients check the list and choose the Group Update Providers that are located in their own subnet. Configuring multiple Group Update Providers turns multiple clients into Group Update Providers. Use multiple Group Update Providers for any of the following scenarios: • You have multiple groups and want to use different Group Update Providers for each group. You can use one policy that specifies rules for the election of multiple Group Update Providers. If clients change locations, you do not have to update the LiveUpdate Settings policy. The Symantec Endpoint Protection Manager combines multiple Group Update Providers across sites and domains. It makes the list available to all clients in all groups in your network. • Multiple Group Update Providers can function as a failover mechanism. The use of Multiple Group Update Providers ensures a higher probability that at least one Group Update Provider is available in each subnet.
Explicit list	Use an explicit list of Group Update Providers when you want clients to be able to connect to Group Update Providers that are on subnets other than the client's subnet. Clients that change location can roam to the closest Group Update Provider on the list. An explicit Group Update Providers list does not turn clients into Group Update Providers. When you configure an explicit list, you can specify that the clients with IP addresses that fall on a particular subnet should use a particular Group Update Provider. A client may have multiple IP addresses, and the management server considers all of the client's IP addresses when it matches which Group Update Provider to use. So, the IP address that the policy matches to is not necessarily bound to the interface that the client uses to communicate with the Group Update Provider. For example, suppose that a client has IP address A, which it uses to communicate with the management server and with the Group Update Provider. This same client also has IP address B, which is the one that matches the Explicit Group Update Provider that you have configured in the LiveUpdate Settings policy for this client. The client can choose to use a Group Update Provider based on the address B, even though that is not the address that it uses to communicate with the Group Update Provider.

Configuring single or multiple Group Update Providers in a LiveUpdate Settings policy performs the following functions:

- It specifies which clients with this policy are to act as Group Update Providers.
- It specifies which Group Update Providers the clients with this policy should use for content updates.

Configuring an explicit Group Update Provider list performs only one function:

- It specifies which Group Update Providers the clients with this policy should use for content updates. Although it does not turn clients into Group Update Providers, you can still configure and apply a policy that contains only an explicit provider list. However, you must then have a single Group Update Provider or multiple Group Update Providers configured in another policy in the Symantec Endpoint Protection Manager. Or, you can have both types configured in other policies.

If a client cannot obtain its update through any of the Group Update Providers, it can then optionally try to update from the Symantec Endpoint Protection Manager.

More information

- [About the effects of configuring more than one type of Group Update Provider in your network](#)
- [Using Group Update Providers to distribute content to clients](#)
- [Configuring clients to download content from Group Update Providers](#)
- [Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager](#)

Configuring Windows clients to download content from Group Update Providers

You use the LiveUpdate Settings policy so that Windows clients get updates from the Group Update Provider only and never from the management server. You can set up single, multiple, or cross-subnet Group Update Providers. The type of Group Update Provider that you set up depends on your network and the clients on that network. See:

[About the types of Group Update Providers](#)

Mac clients and Linux clients cannot get content from a Group Update Provider.

To configure Windows clients to download content from Group Update Providers

1. To configure clients to download content from Group Update Providers, in the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, right-click the policy that you want and then click **Edit**.
4. In the **LiveUpdate Settings Policy** window, under **Windows Settings**, click **Server Settings**.
5. Under **Internal or External LiveUpdate Server**, check **Use the default management server**.
6. Under **Group Update Provider**, check **Use a Group Update Provider**.
7. Click **Group Update Provider**.
8. Do one of the following tasks:
 - Follow the steps in [To configure a single Group Update Provider](#).
 - Follow the steps in [To configure multiple Group Update Providers](#).
 - Follow the steps in [To configure an explicit list of Group Update Providers](#).
9. Under **Group Update Provider Settings**, configure the options to control how content is downloaded and stored on the Group Update Provider computer.
Click **Help** for information about content downloads.
10. Click **OK**.

To configure a single Group Update Provider

1. In the **Group Update Provider** dialog box, check **Single Group Update Provider IP address or host name**, and type the IP address or host name of the client computer that acts as the single Group Update Provider.
Click **Help** for information about the IP address or host name.
2. Return to the procedure to configure a Group Update Provider.

To configure multiple Group Update Providers

1. In the **Group Update Provider** dialog box, check **Multiple Group Update Providers**, and then click **Configure Group Update Provider List**.
2. In the **Group Update Provider List** dialog box, select the tree node **Group Update Provider**, and then click **Add** to add a rule set.
3. In the **Specify Group Update Provider Rule Criteria** dialog box, in the **Check** drop-down list, select one of the following options:
 - **Computer IP Address or Host Name**
 - **Registry Keys**
 - **Operating System**
4. If you selected **Computer IP Address or Host Name** or **Registry Keys**, click **Add**.
5. Type or select the IP address or host name, Windows registry key, or operating system information. Click **Help** for information on configuring rules.
6. Click **OK** until you return to the **Group Update Provider List** dialog box, where you can optionally add more rule sets.
7. Click **OK**.
8. Return to the procedure to configure a Group Update Provider.

To configure an explicit list of Group Update Providers

1. In the **Group Update Provider** dialog box, check **Explicit Group Update Providers for roaming clients**, and then click **Configure Explicit Group Update Provider List**.
2. Click **Add**.
3. In the **Add Explicit Group Update Provider** dialog box, type the client subnet that you want to map these Group Update Providers to.
Click **Specify Client Subnet Mask** to add multiple client subnets at one time. See:
[Add Explicit Group Update Provider](#)
4. Select the **Type** of mapping you want to set up: based on the IP address, the host name, or the Group Update Provider's network address.
Type in the necessary settings for the type of mapping you selected.
5. Click **OK**.

More information

- [Choose a distribution method to update content on clients](#)
- [Using Group Update Providers to distribute content to clients](#)

Searching for the clients that act as Group Update Providers

You can verify that clients are available as Group Update Providers. You can view a list of Group Update Providers by searching for them on the **Clients** tab.

NOTE

You can also check a client's properties. The properties include a field that indicates whether or not the client is a Group Update Provider.

To search for the clients that act as Group Update Providers

-
1. In the console, click **Clients**.
 2. On the **Clients** tab, in the **View** box, select **Client status**.
 3. In the **Tasks** pane, click **Search clients**.
 4. In the **Find** drop-down list, select **Computers**.
 5. In the **In Group** box, specify the group name.
 6. Under **Search Criteria**, click in the **Search Field** column and select **Group Update Provider**.
 7. Under **Search Criteria**, click in the **Comparison Operator** column and select **=**.
 8. Under **Search Criteria**, click in the **Value** column and select **True**.
Click **Help** for information on the search criteria.
 9. Click **Search**.

More information

[Using Group Update Providers to distribute content to clients](#)

Configuring multiple types of Group Update Providers in your network

When you configure single or multiple Group Update Providers in policies, then Symantec Endpoint Protection Manager constructs a global list of all the providers that have checked in. By default, this file is:

- **32-bit operating systems:** `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml`.
- **64-bit operating systems:** `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml`

Symantec Endpoint Protection Manager provides this global list to any client that asks for it so that the client can determine which Group Update Provider it should use. Because of this process, clients that have policies with only multiple or explicit Group Update Providers configured can also use single Group Update Providers, if the single provider meets the explicit mapping criterion. This phenomenon can occur because single providers are a part of the global list of providers that the clients get from their Symantec Endpoint Protection Manager.

So, all of the Group Update Providers that are configured in any of the policies on a Symantec Endpoint Protection Manager are potentially available for clients' use. If you apply a policy that contains only an explicit Group Update Provider list to the clients in a group, all of the clients in the group attempt to use the Group Update Providers that are in the Symantec Endpoint Protection Manager global Group Update Provider list that meet the explicit mapping criteria.

NOTE

A Symantec Endpoint Protection client may have multiple IP addresses. Symantec Endpoint Protection considers all IP addresses when it matches to a Group Update Provider. So, the IP address that the policy matches is not always bound to the interface that the client uses to communicate with the Symantec Endpoint Protection Manager and the Group Update Provider.

If all types of Group Update Providers are configured in the policies on a Symantec Endpoint Protection Manager, then clients try to connect to Group Update Providers in the global list in the following order:

- Providers on the **Multiple Group Update Providers** list, in order
- Providers on the **Explicit Group Update Providers** list, in order
- The Provider that is configured as a **Single Group Update Provider**

You can configure the following types of explicit mapping criteria:

-
- IP address: Clients in subnet A should use the Group Update Provider that has the IP address `x.x.x.x`.
 - Host name: Clients in subnet A should use the Group Update Provider that has the host name `xxxx`.
 - Subnet network address: Clients in subnet A should use any Group Update Provider that resides on `subnet B`.

Multiple mapping criteria can be used in an explicit Group Update Provider list in a single policy. Symantec recommends that you be very careful how you configure multiple mapping criteria to avoid unintended consequences. For example, you can strand your clients without a means of obtaining updates if you misconfigure an explicit mapping.

Consider a scenario with the following multiple explicit mapping criteria configured in a single policy:

- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.24
- If a client is in subnet 10.1.2.0, use the Group Update Provider that has IP address 10.2.2.25
- If a client is in subnet 10.1.2.0, use the Group Update Provider that has host name `SomeMachine`
- If a client is in subnet 10.1.2.0, use any Group Update Provider on subnet 10.5.12.0
- If a client is in subnet 10.6.1.0, use any Group Update Provider on subnet 10.10.10.0

With this explicit Group Update Provider policy, if a client is in subnet 10.1.2.0, the first four rules apply; the fifth rule does not. If the client is in a subnet for which no mapping is specified, such as 10.15.1.0, then none of the rules apply to that client. That client's policy says to use an explicit Group Update Provider list, but there is no mapping that the client can use based on these rules. If you also disabled that client's ability to download updates from Symantec Endpoint Protection Manager and the Symantec LiveUpdate server, then that client has no usable update method.

More information

- [About the types of Group Update Providers](#)
- [Configuring clients to download content from Group Update Providers](#)

Using Intelligent Updater files to update content on Symantec Endpoint Protection clients

Symantec recommends that client computers use LiveUpdate to update content on Symantec Endpoint Protection clients. However, if you do not want to use LiveUpdate or if LiveUpdate is not available, you can use an Intelligent Updater file to update clients. The Intelligent Updater .exe files for Windows are designed to update the clients only. Intelligent Updater files do not contain the information that Symantec Endpoint Protection Manager needs to update its managed clients.

The Intelligent Updater file for Windows is a self-executing file that contains virus and spyware definitions. Additional Intelligent Updater files are available for SONAR definitions, and for intrusion prevention signatures. For Mac and for Linux, you can download virus and spyware definitions.

After you download the file, you can use your preferred distribution method to distribute the updates to your clients.

NOTE

An Intelligent Updater file does not provide updates for any other type of content. For example, Intelligent Updater does not support the extended file attributes and signatures, the Auto-Protect portal list, Power Eraser definitions, or reduced-size definitions.

To use Intelligent Updater files to update content on Symantec Endpoint Protection clients

1. To download an Intelligent Updater file, using your web browser, go to the following page:
[Virus Definitions & Security Updates](#)
2. From the drop-down list, select one of the available Symantec Endpoint Protection options.
The page refreshes to display the content available for that version.

3. In a protection category, next to **Download**, click **Definitions**.
4. Click the appropriate file name for the version of the client you want to update.

NOTE

For Linux virus definitions, click the **Unix Platforms** tab.

5. When you are prompted for a location in which to save the file, select a folder on your hard drive.
6. Distribute the file to the client computers using your preferred distribution method.
7. To install the virus definitions and security updates files on a client computer, on the client computer, locate the Intelligent Updater file that was distributed to the client.
8. Do one of the following:
 - For Windows: Double-click the .exe file, and then follow the on-screen instructions.
 - For Mac: Double-click the .zip file, double-click the .pkg file, and then follow the on-screen instructions.
 - For Linux: Verify that the file has executable permissions, verify that uudecode and uncompress are installed, and then run the .sh file with superuser privilege. See the following for more information:
[How to update a Linux-based computer with Intelligent Updater definitions](#)

More information

[Choose a distribution method to update content on clients](#)

Using third-party distribution tools to update client computers

Some large enterprises rely on third-party distribution tools like IBM Tivoli or Microsoft SMS to distribute content updates to client computers. Symantec Endpoint Protection supports the use of third-party distribution tools to update the managed and unmanaged clients that run Windows operating systems. Mac and Linux clients can only receive content updates from internal or external LiveUpdate servers.

Before you set up the use of third-party distribution tools, you must have already installed Symantec Endpoint Protection Manager and the client computers that you want to update.

Table 166: Tasks to set up the use of third-party distribution tools for updates

Task	Description
Configure Symantec Endpoint Protection Manager to receive content updates.	You can configure the management server either to receive content updates automatically or manually. See: • Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager • How to update content and definitions on the clients
Configure the group's LiveUpdate Settings policy to allow third-party content update distribution.	If you want to use third-party distribution tools to update managed clients, you must configure the group's LiveUpdate Settings policy to allow it. See: Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients
Prepare unmanaged clients to receive updates from third-party distribution tools.	If you want to use third-party distribution tools to update unmanaged clients, you must first create a registry key on each unmanaged client. See: Preparing unmanaged clients to receive updates from third-party distribution tools

Task	Description
Locate, copy, and distribute the content.	Each Symantec Endpoint Protection Manager client group has an index2.dax file that is located on the computer that runs Symantec Endpoint Protection Manager. These files are located by default in subfolders under the <code>SEPM_Install\data\outbox\agent</code> folder. To update clients, you need to use the index2.dax files. The default location for <code>SEPM_Install</code> is <code>C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager</code>. See: • Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager • Distributing the content using third-party distribution tools

Configuring a LiveUpdate Settings policy to allow third-party content distribution to managed clients

If you want to use third-party distribution tools to update managed clients, you must configure the client group's LiveUpdate Settings policy to allow it. You can choose whether to disable the ability of client users to manually perform LiveUpdate.

When you are finished with this procedure, a folder appears on the group's client computers in the following location (for Vista and later operating systems):

`C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox`

To enable third-party content distribution to managed clients with a LiveUpdate policy

1. In the console, click **Policies**.
2. Under **Policies**, click **LiveUpdate**.
3. On the **LiveUpdate Settings** tab, under **Tasks**, click **Add a LiveUpdate Setting Policy**.
4. In the **LiveUpdate Policy** window, in the **Policy name** and **Description** text boxes, type a name and description.
5. Under **Windows Settings**, click **Server Settings**.
6. Under **Third Party Management**, check **Enable third party content management**.
7. Uncheck all other LiveUpdate source options.
8. Click **OK**.
9. In the **Assign Policy** dialog box, click **Yes**.
Optionally, you can cancel out of this procedure and assign the policy at a later time.
10. In the **Assign LiveUpdate Policy** dialog box, check one or more groups to which to assign this policy, and then click **Assign**.

More information

[Configuring clients to download content from an internal LiveUpdate server](#)

Preparing unmanaged clients to receive updates from third-party distribution tools

If you install unmanaged clients from the installation file, you cannot immediately use third-party distribution tools to distribute LiveUpdate content or policy updates to them. As a security measure, by default these client computers do not trust or process the content that third-party distribution tools deliver to them.

To successfully use third-party distribution tools to deliver updates, you must first create a Windows registry key on each of the unmanaged clients. The key lets you use the inbox folder on unmanaged clients to distribute LiveUpdate content and policy updates by using third-party distribution tools.

The inbox folder appears on unmanaged clients in the following location (Vista and later operating systems):

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox

Once you create the registry key, you can use a third-party distribution tool to copy content or policy updates to this folder. The Symantec Endpoint Protection client software then trusts and processes the updates.

To prepare unmanaged clients to receive updates from third-party distribution tools

1. On each client computer, use regedit.exe or another Windows registry editing tool to add one of the following Windows registry keys:
 - On 32-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState
 - On 64-bit computers (14.3 RU4 or earlier clients): HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState
 - On 64-bit computers (14.3 RU5 or later clients): HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState
2. Set the value type of the registry key to DWORD (32-bit) or QWORD (64-bit) and the value to hexadecimal 80 as follows:

0x00000080 (128)
3. Save the registry key, and then exit the registry editing tool.

More information

- [Using third-party distribution tools to update client computers](#)
- [Distributing the content using third-party distribution tools](#)

Distributing the content using third-party distribution tools

To use third-party distribution tools to distribute content to client computers, you need to use the index2.dax file. The LiveUpdate-related content in the index2 file includes a set of GUIDs called content monikers and their associated sequence numbers. Each content moniker corresponds to a particular content type. Each sequence number in the index2 file corresponds to a revision of a particular content type. Depending on the protection features that you have installed, you need to determine which of the content types you need. See:

[About the types of content that LiveUpdate downloads](#)

NOTE

Content monikers typically change with each major release. At times, they may also change for a minor release. Symantec does not typically change the monikers for Release Updates or Maintenance Patches.

You can see a mapping of the moniker to its content type by opening the ContentInfo.txt file. By default, the ContentInfo.txt file is located in C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Inetpub\content\.

For example, you might see the following entry:

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SEPC Virus Definitions  
Win32 14.3 RU3 - MicroDefsB.CurDefs - SymAllLanguages
```

Each Symantec Endpoint Protection Manager client group has its own index2 file. The index2 file for each client group is found in a folder for that group. By default, the folders for client groups are found in C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\outbox\agent\. The folder name for a client group corresponds to the group policy serial number. You can find the serial number in the **Group Properties** dialog box or on the **Clients** page **Details** tab. The first four hexadecimal values of each group policy serial number match the first four hexadecimal values of that group's folder.

The index2.dax file that managed clients use is encrypted. To look at the contents of the file, open the index2.xml file that is available in the same folder. The index2.xml file provides a list of the content monikers and their sequence (revision) numbers. For example, you might see the following entry:

```
<File Checksum="D5ED508E8CF7A8A4450B0DBA39BCCB25" DeltaFlag="1"
FullSize="625203112" LastModifiedTime="1425983765211" Moniker=
"{535CB6A4-441F-4e8a-A897-804CD859100E}" Seq="150309034"/>
```

The LiveUpdate Content policy for a group specifies either a particular revision of content or the latest content. The sequence number in the index2 file must match the sequence number that corresponds to the content specification in the group's LiveUpdate Content policy. For example, if the policy is configured to **Use latest available** for all content types, then the sequence number for each type is the latest available content. In this example, the distribution only works if the index2 file calls out the sequence numbers (revisions) that correspond to the latest content revision. The distribution fails if the sequence numbers correspond to any other revisions.

NOTE

You must use the Copy command to place files into the client's \inbox folder. Using the Move command does not trigger update processing, and the update fails. If you compress content into a single archive for distribution, you should not unzip it directly into the \inbox folder.

To distribute content to clients with third-party distribution tools

1. On the computer that runs the Symantec Endpoint Protection Manager, create a working folder such as \Work_Dir.
2. Do one of the following actions:
 - For a managed client, in the console, on the **Clients** tab, right-click the group to update, and then click **Properties**.
 - For an unmanaged client, in the console, on the **Clients** tab, right-click **My Company**, and then click **Properties**.
3. Write down the first four hexadecimal values of the **Policy Serial Number**, such as 7B86.

4. Navigate to the following folder:

```
SEPM_Install\data\outbox\agent
```

Where SEPM_Install represents the installation folder for Symantec Endpoint Protection Manager. The default installation folder is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

5. Locate the folder that contains the first four hexadecimal values that match the **Policy Serial Number**.
6. Open that folder, and then copy the index2.dax file to your working folder.
7. Navigate to the following folder:

```
SEPM_Install\Inetpub\content
```

Where SEPM_Install represents the installation folder for Symantec Endpoint Protection Manager. The default installation folder is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

8. Open and read ContentInfo.txt to discover the content that each target moniker folder contains.

The contents of each directory are in the following format: target moniker\sequence number\full.zip|full.

9. Copy the contents of each \target moniker folder to your working folder such as \Work_Dir.
10. Delete all files and folders from each \target moniker so that only the following folder structure and file remain in your working folder:

```
\\Work_Dir\target moniker\latest sequence number\full.zip
```

Your working folder now contains the folder structure and files to distribute to your clients.

-
11. Use your third-party distribution tools to distribute the content of your working folder to the \\Symantec Endpoint Protection\\inbox\\ folder on each of the clients.

The end result must look like the following:

```
\\Symantec Endpoint Protection\\inbox\\index2.dax
```

```
\\Symantec Endpoint Protection\\inbox\\target moniker\\latest sequence number\\full.zip
```

Files that are processed successfully are then deleted. Files that are not processed successfully are moved to a subfolder named Invalid. If you see files in an **Invalid** folder under the **inbox** folder, then you must try again with those files.

More information

- [Using third-party distribution tools to update client computers](#)
- [Preparing unmanaged clients to receive updates from third-party distribution tools](#)

Monitoring, Reporting, and Enforcing Compliance

Learn how to run and read reports and logs, and set up Host Integrity.

This section describes how to:

- Set up Host Integrity to ensure that client computers are protected and compliant with your company's security policies.
- Use logs and reports to monitor the security in your environment.
- Manage notifications.

Configuring Host Integrity

Use Host Integrity policies to make sure that the Windows client computers in your network meet your organization's security policies.

NOTE

Host Integrity is not supported on Mac clients or Linux agents.

The following table lists the steps to set up security compliance using Host Integrity policies.

Table 167: Tasks to set up Host Integrity policies

Step	Description
Step 1: Create a Host Integrity policy that checks for a requirement on the client computer and enforces a remediation action for non-compliant computers.	To add requirements to a Host Integrity policy 1. In the console, open a Host Integrity policy, and click Requirements. Add the requirements that you want the client computer to check. Create a separate requirement for each type of software (such as applications, files, and patches). See: — Adding predefined requirements to a Host Integrity policy — About Host Integrity requirements 2. In the Add Requirement dialog box, configure the remediation actions for non-compliant client computers. Remediation requires that the client computer installs or requests the client user to install the required software. See: Setting up remediation for a predefined Host Integrity requirement 3. On the Requirements page, use the Move Up and Move Down options to set the order in which requirements are checked and the remediation is tried. For example, updates should be completed in a specific order so that all updates are applied before the user has to restart the client computer.
Step 2: Set the options for the Host Integrity check and notifications.	On the Advanced Settings page: • Configure how often the Host Integrity check runs. See: Configuring the frequency of Host Integrity check settings • Configure whether users can cancel the remediation. See: Allowing users to delay or cancel Host Integrity remediation • Set up a notification to appear on the client computer when the Host Integrity check either passes or fails. Use the notification to tell the end user what to do next. For example, the end user may need to download and install a new patch on the client computer. See: Configuring notifications for Host Integrity checks

Step	Description
Step 3: Set up peer-to-peer enforcement (optional).	If the client computers being tested for Host Integrity compliance are on the same network as already-compliant client computers, you can set up peer-to-peer enforcement. You primarily use peer-to-peer enforcement for file sharing. See: Blocking a remote computer by configuring peer-to-peer authentication
Step 4: Set up a Quarantine policy for non-compliant and unremediated computers (optional).	If the client computer fails the Host Integrity check and does not perform remediation, you can quarantine the computer using a Quarantine policy. See: Creating a Quarantine policy for a failed Host Integrity check

[Generating a list of computers where a Host Integrity check failed](#)

How Host Integrity works

Host Integrity ensures that client computers are protected and compliant with your company's security policies. You use Host Integrity policies to define, enforce, and restore the security of clients to secure enterprise networks and data.

Requirements

For the Host Integrity check to run, make sure that:

- You installed the **Virus, Spyware, and Basic Download Protection** component and the **Firewall** component on the client computer. See:
[Choosing which security features to install on the client](#)
- The **Virus and Spyware Protection** component and the **Network and Threat Protection** component are enabled on the client computer. If the client user disables either of these features, the client computer ignores the Host Integrity policy.

To check that components are enabled

- In the console, add a Host Integrity policy and add a Antivirus, Antispyware, and Firewall requirement.
- For each requirement for **<Antivirus> application that must be installed and running**, select **Symantec Endpoint Protection**.
- Check **Start antivirus if it is not running on the client**.

 Add Requirement
 ✕

Name:

Client Type:

Antivirus application that must be installed and running: Symantec Endpoint Protection ▼

☐ Install antivirus if it has not been installed on the client

☐ Download the installation package

Download URL:

 Execute the command (use %F% to specify the downloaded file if it is available):

☒ Start antivirus if it is not running on the client

Execute the command:

Antivirus Signature File Checking

☐ Specify the oldest age of the signature file: weeks ▼

☐ Check the signature file date

☒ Ensure signature file date is not equal to

☐ Ensure signature file date is equal to

Host Integrity workflow

Table 168: Process for enforcing security compliance on the client computer

Step	Description
Step 1: The client computer runs a Host Integrity check on the client computer.	The management server downloads the Host Integrity policy to the client computers in the assigned group. The client computers run the Host Integrity check, which compares each computer's configuration with the requirements that you add to the Host Integrity policy. The Host Integrity policy checks for the existence for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check whether the latest patches have been applied to the operating system. See: Configuring Host Integrity
Step 2: The Host Integrity check passes or fails	- If the computer meets all of the policy's requirements, the Host Integrity check passes. - If the computer does not meet all of the policy's requirements, the Host Integrity check fails. You can also set up the policy to ignore a failed requirement so that the check passes. See: Allowing the Host Integrity check to pass if a requirement fails You can also set up peer-to-peer authentication in the Firewall policy, which can grant or block inbound access to the remote computers that have the client installed. See: Blocking a remote computer by configuring peer-to-peer authentication

Step	Description
Step 3: Non-compliant computers remediate a failed Host Integrity check (optional)	- If the Host Integrity check fails, you can configure the client to remediate. To remediate, the client downloads and installs the missing software. You can configure either the client to remediate or the end user to remediate in a predefined requirement or a custom requirement. Host Integrity then rechecks that the client computer installed the software. See: Setting up remediation for a predefined Host Integrity requirement - If the Host Integrity check that verifies remediation still fails, the client applies a Quarantine policy. You can use a Quarantine policy to apply stricter restrictions to the failed computers. See: Creating a Quarantine policy for a failed Host Integrity check - While the client is in the Quarantine location, the Host Integrity check continues to run and to try to remediate. The frequency of the check and remediation settings are based on how you configure the Host Integrity policy. Once the client is remediated and passes the Host Integrity check, the client moves out of the Quarantine location automatically. In some cases, you may need to remediate the client computer manually.
Step 4: The client continues to monitor compliance	The Host Integrity check actively monitors each client's compliance status. If at any time the client's compliance status changes, so do the privileges of the computer. - If you change a Host Integrity policy, it is downloaded to the client at the next heartbeat. The client then runs a Host Integrity check. - If the client switches to a location with a different Host Integrity policy while a Host Integrity check is in progress, the client stops checking. The stop includes any remediation attempts. The user may see a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location. You can view the results of the Host Integrity check in the Compliance log. See: Viewing logs

About Host Integrity requirements

When you create a new Host Integrity policy, decide which type of requirements to add.

Each requirement specifies the following items:

- What conditions to check
For example, a requirement would check whether the latest set of virus definitions is installed on the client computer.
- What remediation actions the client takes if the client fails to pass the condition's requirements
For example, the remediation action can include a URL where the client can download and install the missing virus definitions.

The following table lists the types of requirements you can use.

Table 169: Requirement types for Host Integrity policies

Type	Description
Predefined requirements	Use a predefined requirement to check that a specific application or file is installed and runs on the client. A predefined requirement checks for the status of any of the following types of applications: antivirus software, antispyware software, a firewall, a patch, or a service pack. For example, a patch requirement checks that the client computers run a specific operating system patch. If the predefined requirement does not have enough detail, add a custom requirement and write a script. See: Adding predefined requirements to a Host Integrity policy
Custom requirements from templates	Templates are predefined custom requirements that Symantec wrote for commonly performed tasks. For example, the client can check that a password has been changed in the last 42 days. You can also use the templates as a basis for writing a custom requirement script. Template requirements are available through the Host Integrity policy LiveUpdate service. You must first set up LiveUpdate to download the Host Integrity templates to the management server. See: • Adding a custom requirement from a template • Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager
Custom requirements	Use a custom requirement if neither a predefined requirement nor the templates provide the kind of check that you need. Custom requirements include the same fields as predefined requirements, but provide more flexibility. For example, you can include an antispyware application that is not included in the predefined list of antispyware applications. You can simplify the management of required applications by including similar applications in one custom requirement. For example, you can include Internet browsers such as Internet Explorer and Mozilla Firefox in one requirement. See: Writing a customized requirement script

More information

[Setting up Host Integrity](#)

Adding predefined requirements to a Host Integrity policy

A predefined requirement in a Host Integrity policy checks that the client computer runs any of several types of applications such as antivirus, antispyware, or a firewall.

You determine the particular application, such as specific patches for the Windows 7 operating system. You then specify the path where the client computers should get the patch.

To add predefined requirements to a Host Integrity policy

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
4. Configure the settings and remediation options for the requirement, and then click **OK**. See: [Setting up remediation for a predefined Host Integrity requirement](#)

More information

- [Adding a custom requirement from a template](#)
- [Writing a customized requirement script](#)

Setting up remediation for a predefined Host Integrity requirement

If the Host Integrity check on a client shows that a requirement failed, you can configure the policy to restore the necessary files. The client restores files by downloading, installing, or running the required applications to meet the requirement. The client computer can then pass the Host Integrity check.

You set up remediation in the same dialog box in which you add a predefined requirement. You specify both the path from which the client downloads the remediation files and how the remediation process is implemented.

You can also enable users to have some control over when they remediate their computers. For example, a restart may cause users to lose their work, so users may want to delay remediation until the end of the day.

After the download, installation, or execution of a command to restore a requirement, the client always retests the requirement. Also, the client logs the results as `pass` or `fail`.

To set up remediation for a predefined Host Integrity requirement

1. In the console, open a Host Integrity policy, and add a predefined requirement. See:

[Adding predefined requirements to a Host Integrity policy](#)

2. In the **Add Requirement** dialog box, click **Install the <requirement type> if it has not been installed on the client**.
3. Click **Download the installation package**.
4. In the **Download URL** text box, type the URL from where the installation file gets downloaded to the client computer. See:

[About specifying the file location and execute command for remediation](#)

5. In the **Execute the command** text box, do one of the following tasks:

- If you want the client user to run the installation, leave the text box blank.
- If you want the installation to run automatically, type `%F%`.

The `%F%` variable represents the last downloaded file. You can use any command that can be run from **Start > Run**. For example, to install a patch for Vista, type the command `%Systemroot%\system32\wusa.exe /quiet /norestart %F%`.

6. Optionally set the options to delay or cancel remediation, and then click **OK**. See:

[Allowing users to delay or cancel Host Integrity remediation](#)

7. Click **OK**.

More information

[Allowing the Host Integrity check to pass if a requirement fails](#)

Allowing users to delay or cancel Host Integrity remediation

You can allow the user to delay remediation to a more convenient time. If users must restart their computers after they install the software for a requirement, they may want to wait to restart their computers until later.

If the user delays remediation, any of the following events can happen:

- The client logs the event. The Host Integrity status is shown as failed because the requirement is not met. The user can manually run a new Host Integrity check at any time from the client.
- The Host Integrity check remediation message window does not appear again until the client runs another Host Integrity check. If the user has chosen to be reminded in five minutes, but the Host Integrity check runs every 30

minutes, the message window does not appear until 30 minutes. To avoid confusion for the user, you may want to synchronize the minimum time setting with the Host Integrity check frequency setting.

- If the user delays the remediation before the next Host Integrity check, the user selection is overridden.
- If the user delays a remediation action and the client receives an updated policy, the amount of time available for remediation is reset to the new maximum.

To allow users to delay or cancel Host Integrity remediation

1. In the console, open a Host Integrity policy and add a requirement. See:
[Adding predefined requirements to a Host Integrity policy](#)
2. In the **Add Requirement** dialog box, set up remediation. See:
[Setting up remediation for a predefined Host Integrity requirement](#)
3. On the dialog box for the requirement, do one of the following tasks, and then click **OK**:
 - To let the client user delay a file from being downloaded, check **Specify wait time before attempting the download again if the download fails**.
 - To let the client user cancel remediation, check **Allow the user to cancel the download for Host Integrity remediation**.
4. Click **OK**.
5. Click **Advanced Settings**.
6. On the **Advanced Settings** page, under **Remediation Dialog Options**, configure the options for canceling the remediation.
7. To add a custom message on the client computer, click **Set Additional Text**.
The message you type appears on the client remediation window if the user clicks **Details**.
8. Click **OK**.

Configuring the frequency of Host Integrity check settings

You can configure how the Host Integrity check is carried out and how the results are handled.

After you add or update a Host Integrity policy, the policy is downloaded to the client at the next heartbeat. The client then runs the Host Integrity check.

If the user switches to a location with a different policy while a Host Integrity check is in progress, the client stops the check. The stop includes remediation attempts, if required by the policy. The user may get a timeout message if a remediation server connection is not available in the new location. When the check is complete, the client discards the results. Then the client immediately runs a new Host Integrity check based on the new policy for the location.

If the policy is the same in the new location, the client maintains any Host Integrity timer settings. The client runs a new Host Integrity check only when required by the policy settings.

To configure the frequency of Host Integrity check settings

1. In the console, open a Host Integrity policy, and click **Advanced Settings**.
2. On the **Advanced Settings** page, under **Host Integrity Checking Options**, set the Host Integrity check frequency.
3. Click **OK**.

More information

- [Adding predefined requirements to a Host Integrity policy](#)
- [Allowing the Host Integrity check to pass if a requirement fails](#)

Allowing the Host Integrity check to pass if a requirement fails

Users may need to continue working even if their computers fail the Host Integrity check. You can let the Host Integrity check pass even if a specific requirement fails. The client logs the results but ignores the results.

You apply this setting for a specific requirement. If you want to apply this setting to all requirements, you must enable the setting on each requirement separately. The setting is disabled by default.

To allow the Host Integrity check to pass if a requirement fails

1. In the console, open a Host Integrity policy.
2. Add a predefined requirement or a custom requirement, and then click **OK**. See:
 - [Adding predefined requirements to a Host Integrity policy](#)
 - [Writing a customized requirement script](#)
3. On the dialog box for the requirement, check **Allow the Host Integrity check to pass even if this requirement fails**, and then click **OK**.
4. Click **OK**.

Configuring notifications for Host Integrity checks

When the client runs a Host Integrity check, you can configure notifications to appear when the following conditions occur:

- A Host Integrity check fails.
- A Host Integrity check passes after it previously failed.

The results of the Host Integrity check appear in the client's Security log. They are uploaded to the Compliance log on the **Monitors** page of the management server.

The client's Security log contains several panes. If you select a Host Integrity check event type, the lower left-hand pane lists whether the individual requirement has passed or failed. The lower right-hand pane lists the conditions of the requirement. You can configure the client to suppress the information in the lower right-hand pane. Although you may need this information when troubleshooting, you may not want users to view the information. For example, you may write a custom requirement that specifies a registry value or a file name. The details are still recorded in the Security log.

You can also enable a notification that gives the user the choice to download the software immediately or delay the remediation. See:

[Allowing users to delay or cancel Host Integrity remediation](#)

To configure notifications for Host Integrity checks

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity** page, click **Advanced Settings**.
3. On the **Advanced Settings** page, under **Notifications**, to show detailed requirement information, check **Show verbose Host Integrity Logging**.

The lower right-hand pane of the client's Security log displays complete information about a Host Integrity requirement.

4. Check any of the following options:
 - **Display a notification message when a Host Integrity check fails.**
 - **Display a notification message when a Host Integrity check passes after previously failing.**

-
5. To add a custom message, click **Set Additional Text**, type up to 512 characters of additional text, and then click **OK**.
 6. When you are finished with the configuration of this policy, click **OK**.

Creating a Quarantine policy for a failed Host Integrity check

You use a Quarantine policy for the client computers that fail the Host Integrity check, try to remediate, and then fail remediation again. After the client computer fails remediation, it automatically switches to a Quarantine location, where a Quarantine policy is applied to the computer. You use a Quarantine policy to apply stricter restrictions to the failed computers. You can use any type of protection policy for the Quarantine policy. For example, you can apply a Quarantine Firewall policy that blocks a computer's access to the Internet.

While the client computer is in the Quarantine location, you can configure the Host Integrity check to continue to run and try to remediate the computer. You may also need to remediate the computer manually.

To create a Quarantine policy for a failed Host Integrity check

1. In the console, click **Clients**, and then click the **Policies** tab.
2. On the **Policies** tab, next to **Quarantine Policies when Host Integrity Fails**, click **Add a policy**.
3. In the **Add Quarantine Policy** dialog box, choose a policy type and then click **Next**.
4. Choose whether to use an existing policy, create a new policy, or import a policy file, and then click **Next**.
5. Do one of the following tasks:
 - In the **Add Policy** dialog box, choose the policy, and click **OK**.
 - In the **Policy Type** dialog box, configure the policy, and click **OK**.
 - In the **Import Policy** dialog box, locate the `.dat` file and click **Import**.

More information

- [Setting up remediation for a predefined Host Integrity requirement](#)
- [About Host Integrity requirements](#)

Generating a list of computers where a Host Integrity check failed

After you create a Host Integrity policy to check whether a requirement passes, you'll want to know which clients are failing the Host Integrity check. For example, you may want to know whether a Microsoft patch is installed.

To view a report of the computers on which a Host Integrity check has failed

1. In the console, click the **Home**.
2. Under **Endpoint Status**, click **Host Integrity Failed**.

This Compliance log lists every Host Integrity failed event within the time range given. Use the list to determine which devices in the network still need a Microsoft patch installed.

To generate a list of computers on which a Host Integrity check has failed

1. In the console, click the **Monitors > Logs** tab.
2. In the **Log type** drop-down list, select **Compliance**.
3. In the **Log content** drop-down list, select **Client Host Integrity**.
4. Click **Additional Settings**.
5. Adjust the **Time range**.
6. In the **Event type** drop-down list, select **Host Integrity failed**.
7. Click **View Log**.

Blocking a remote computer by configuring peer-to-peer authentication

You can use peer-to-peer authentication to allow a remote client computer (peer) to connect to another client computer (authenticator) within the same corporate network. The authenticator temporarily blocks inbound TCP and UDP traffic from the remote computer until the remote computer passes the Host Integrity check. You can use this enforcement technique when the remote computer is physically remote. The technique leverages advanced capabilities of the Symantec Endpoint Protection firewall to enhance access to shared files.

The Host Integrity check verifies the following characteristics of the remote computer:

- The remote computer has Symantec Endpoint Protection installed.
- The remote computer passed the Host Integrity check.

If the remote computer passes the Host Integrity check, the authenticator allows inbound connections from the remote computer.

If the remote computer fails the Host Integrity check, the authenticator continues to block the remote computer. You can specify how long the remote computer is blocked before it can try to connect to the authenticator again. You can also specify certain remote computers to always be allowed, even if they do not pass the Host Integrity check. If you do not enable a Host Integrity policy for the remote computer, the remote computer passes the Host Integrity check.

Peer-to-peer authentication information appears in the Network and Host Exploit Mitigation Traffic log.

NOTE

Peer-to-peer authentication works in server control and mixed control, but not in client control.

To block a remote computer by configuring peer-to-peer authentication

1. In the console, open a Firewall policy.
2. On the **Firewall policy** page, click **Peer-to-Peer Authentication Settings**.
3. On the **Peer-to-Peer Authentication Settings** page, check **Enable peer-to-peer authentication**.
4. Configure each value that is listed on the page.

For more information about these options, click **Help**.

5. To allow remote computers to connect to the client computer without being authenticated, check **Exclude hosts from authentication**, and then click **Excluded Hosts**.

The client computer allows traffic to the computers that are listed in the **Host** list.

6. In the **Excluded Hosts** dialog box, click **Add** to add the remote computers that do not have to be authenticated.
7. In the **Host** dialog box, define the host by IP address, IP range, or the subnet, and then click **OK**.
8. In the **Excluded Hosts** dialog box, click **OK**.
9. Click **OK**.
10. If you are prompted, assign the policy to a group.

More information

- [Creating a firewall policy](#)
- [Setting up Host Integrity](#)
- [Preventing users from disabling protection on client computers](#)

Creating Host Integrity policy requirements by importing templates

Use Symantec-provided Host Integrity Policy requirement templates to create SEP Host Integrity Policy requirements.

Instead of creating custom Host Integrity Policy requirements from scratch, you can use pre-defined templates that provide commonly used requirements. A Host Integrity Policy requirement defines (1) a condition that SEP should check, and (2) the remediation to take if the condition fails. For example: A Host Integrity requirement is to check whether a client is using the latest virus definitions. If it is not, the remediation is to send the client an email with a URL where the user can download the current virus definitions.

To obtain the Host Integrity Policy templates, download the Host Integrity content to the management server through LiveUpdate. The Host Integrity content contains the Host Integrity Policy requirement templates.

NOTE

If you download a Host Integrity Policy requirement template and a requirement with the same name exists, SEP does not overwrite your existing requirement. Instead, the new requirement appears on the Requirements table with the number 2 appended to the name.

To creating Host Integrity policy requirements by importing templates

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click **Use existing templates**, and then click **OK**.
4. In the **Host Integrity Online Updating** dialog box, under **Templates**, select a template category.
5. Next to each template you want to add, click **Add**.
6. Click **Import**.
7. Click **OK**.

See:

[About Host Integrity requirements](#)

Writing a customized requirement script

Custom requirements provide more flexibility than a predefined requirement. For example, you can add an application that is not included in the predefined lists of applications.

To build a custom requirement, you add one or more functions or **IF..THEN** statements to a script. When you run the script, the Host Integrity check looks for the condition that is listed under the **IF** node. Depending upon the condition, the action that is listed under the **THEN** node is executed. The result (*pass* or *fail*) is returned.

When you add many different conditions in one script to check for, this setting applies to the entire custom requirement script. This choice may affect whether you want to create several small custom requirements or a longer one that includes multiple steps.

To write a customized requirement script

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
4. In the **Custom Requirement** dialog box, type a name for the requirement.

The requirement name appears on the client computer. The name notifies the user whether the requirement has passed or the requirement has failed or prompts the user to download the software.

-
5. To add a condition, under **Customized Requirement Script**, click **Add**, and then click **IF..THEN**.

NOTE

If you first add a function or an **IF..THEN** statement without filling out the fields, an error appears. If you do not want to add the statement, right-click the statement and click **Delete**.

6. With the highlight on the empty condition under the **IF** node, in the right pane, select a condition.

The Host Integrity check looks for the condition on the client computer.

7. Under the **Select a condition** drop-down list, specify the additional information that is required.

8. Under **Customized Requirement Script**, click **THEN**, and then click **Add**.

The **THEN** statement provides the action that should be taken if the condition is true.

9. Click any of the following options:

- **IF..THEN**
Use a nested **IF..THEN** statement to define conditions to check and actions to take if the condition is evaluated as true.
- **Function**
Use a function to define a remediation action, such as downloading a file.
- **Return**
Use a return statement to specify whether the results of the evaluation of the condition pass or fail. Every custom requirement must end with a pass or fail statement.
- **Comment** (optional)
Use a comment to explain the functionality of the conditions, functions, or statements that you add.

10. In the right-hand pane, define the criteria that you added.

For more information on these options, click **Help**.

11. To add more nested statements, conditions, or functions, under **Customized Requirement Script**, right-click the node, and then click **Add**.

12. Repeat steps 9 to 11 as needed.

13. To allow the Host Integrity check to pass no matter what the result, check **Allow the Host Integrity check to pass even if this requirement fails**.

14. Click **OK**.

More information

- [Creating a test Host Integrity policy with a custom requirement script](#)
- [Adding predefined requirements to a Host Integrity policy](#)

About registry conditions

You can specify which Windows registry settings to check as part of an **IF..THEN** statement for a customized requirement. You can also specify ways to change registry values. Only `HKEY_CLASSES_ROOT`, `HKEY_CURRENT_USER`, `HKEY_LOCAL_MACHINE`, `HKEY_USERS`, and `HKEY_CURRENT_CONFIG` are supported registry settings.

When you specify registry keys, remember the following considerations:

- The key name is limited to 255 characters.
- If the registry key has a backslash (\) at the end, it is interpreted as a registry key. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\`
- If the registry key has no backslash at the end, then it is interpreted as a registry name. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch`

When you specify registry values, remember the following considerations:

- The value name is limited to 255 characters.
- You can check for values as DWORD (decimal), Binary (hexadecimal), or String.
- For DWORD values, you can check whether the value is less than, equal to, not equal to, or greater than the specified value.
- For string values, you can check whether the value data equals or contains a given string. If you want the string comparison to be case-sensitive, check the **Match case** check box.
- For binary values, you can check whether the value data equals or contains a given piece of binary data. Hexadecimal bytes represent the data. If you specify value contains, you can also specify the offset for this data. If the offset is left blank, it searches the value for the given binary data. Allowed values for the hexadecimal edit box are 0 through 9 and a through f.

The following are examples of registry values:

DWORD	12345 (in decimal)
Binary	31 AF BF 69 74 A3 69 (in hexadecimal)
String	ef4adf4a9d933b747361157b8ce7a22f

Writing a custom requirement to run a script on the client

In a custom Host Integrity requirement, you can specify a function that causes the client to run a script. You can use a scripting language, such as JScript or VBScript, which you can run with the Microsoft Windows Script Host.

To write a custom requirement to run a script on the client

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**. See:

[Writing a customized requirement script](#)

4. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
5. Click **Add**, and then click **Function**.
6. Click **Utility: Run a script**.
7. Enter a file name for the script, such as `myscript.js`.
8. Type the content of the script.
9. In the **Execute the command** text field, type the command to use to execute the script.
Use `%F` to specify the script file name. The script executes in system context.
10. To specify the amount of time to allow the **Execute** command to complete, select one of the following options:

- **Do not wait**

The action returns true if the execution is successful but it does not wait until the execution is completed.

- **Wait until execution completes**
- **Enter maximum time**

Enter a time in seconds. If the `Execute` command does not complete in the specified time, the file execution is terminated.

11. Optionally, uncheck **Delete the temporary file after execution is completed or terminated** if you no longer need it.
This option is disabled and unavailable if **Do not wait** is selected.
12. Optionally, uncheck **Show new process window** if you do not want to see a window that shows the requirement running the script.

Writing a custom requirement to set the timestamp of a file

In the custom Host Integrity requirement, you can specify the **Set Timestamp** function to create a Windows registry setting to store the current date and time. You can then use the **Check Timestamp** condition to find out if a specified amount of time has passed since that timestamp was created.

For example, if the Host Integrity check runs every 2 minutes, you can specify an action to occur at a longer interval such as a day. In this case, the stored time value is removed. You could set the script to run as follows:

- When the client receives a new profile
- When the user manually runs a Host Integrity check

To write a custom requirement to set the timestamp of a file

1. In the console, open a Host Integrity policy.
2. On the **Host Integrity policy** page, click **Requirements > Add**.
3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.

[Writing a customized requirement script](#)

4. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
5. Click **Add**, and then click **Function**.
6. Click **Utility: Set Timestamp**.
7. Type a name up to 255 characters long for the registry setting that stores the date and the time information.
For example, enter `Date and time of last file update`:

To compare the current time to the stored time value

1. Write a custom requirement script. For more information, see:
[Writing a customized requirement script](#)
2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the condition.
3. Click **Add**, and then click **IF..THEN**.
4. Click **Utility: Check Timestamp**.
5. Type the name you entered for the saved time registry setting.
6. Specify an amount of time in minutes, hours, days, or weeks.
If the specified amount of time has passed, or if the value of the registry setting is empty, the **Set Timestamp** function returns a value of True.

Writing a custom requirement to increment a registry DWORD value

For a custom requirement, you can increment the Windows registry DWORD value. The **Increment registry DWORD** value function creates the key if it does not exist.

To write a custom requirement to increment the registry DWORD value

1. In the console, add a Host Integrity policy with a custom requirement script. See:

[Writing a customized requirement script](#)

2. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, select the node where you want to add the function.
3. Click **Add**, and then click **Function**.
4. Click **Registry: Increment registry DWORD value**.
5. Enter the registry key to check in the **Registry key** field.
6. Enter a value name to be checked in the **Value name** field.
7. Click **OK**.

Creating a test Host Integrity policy with a custom requirement script

The policy that you create for this test is for demonstration purposes only. The policy detects the existence of an operating system and, when detected, generates a `fail` event. Normally, you would generate `fail` events for other reasons.

Complete the following tasks:

- Add a Host Integrity policy with a custom requirement script that checks for the operating system on the client computer. See:
[To create a test Host Integrity policy with a custom requirement script](#)
- Test the Host Integrity policy you have created. See:
[To test the Host Integrity policy on the client computer](#)

To create a test Host Integrity policy with a custom requirement script

-
1. In the console, open a Host Integrity policy.
 2. On the **Host Integrity policy** page, click **Requirements > Add**.
 3. In the **Add Requirement** dialog box, click the **Select requirement** drop-down list, select a predefined requirement, and then click **OK**.
 4. In the **Name** box, type a name for the custom requirement.
 5. In the **Custom Requirement** dialog box, under **Customized Requirement Script**, right-click **Insert statements below**, and then click **Add > IF..THEN**.
 6. In the right pane, in the **Select a condition** drop-down list, click **Utility: Operating System is**.
 7. Under **Operating system**, check one or more operating systems that your client computers run and that you can test.
 8. Under **Customized Requirement Script**, right-click **THEN //Insert statements here**, and then click **Add > Function > Utility: Show message dialog**.
 9. In the **Caption of the message box** field, type a name to appear in the message title.
 10. In the **Text of the message box** field, type the text that you want the message to display.
 11. In the left pane, under **Customized Requirement Script**, click **Pass**.
 12. In the right pane, under **As the result of the requirement, return**, check **Fail**, and then click **OK**.
 13. Click **OK**.
 14. In the **Host Integrity Policies** dialog box, in the left panel, click **Assign the policy**.
 15. In the **Assign Host Integrity Policy** dialog box, select the groups to which you want to assign the policy, and click **Assign**.

In the **Assign Host Integrity Policy** dialog box, click **Yes** to assign the Host Integrity policy changes.

NOTE

One Host Integrity policy can be assigned to multiple groups, while a single group can only have a single Host Integrity policy. You can replace an existing policy with a different policy.

16. To test the Host Integrity policy on the client computer, in the console, click **Clients > Clients**.
17. Under **Clients**, click and highlight the group that contains the client computers to which you applied the Host Integrity policy.
18. Under **Tasks**, click **Run a command on the group > Update Content**, and then click **OK**.
19. Log on to the computer that runs the client and note the message box that appears.

Because the rule triggered the `fail` test, the message box appears. After testing, disable or delete the test policy.

More information

- [Writing a customized requirement script](#)
- [Writing a custom requirement to increment a registry DWORD value](#)
- [Writing a custom requirement to run a script on the client](#)

Monitoring the Symantec Endpoint Protection clients

Symantec Endpoint Protection collects information about the security events in your network. You can use log and reports to view these events, and you can use notifications to stay informed about the events as they occur.

You can use the reports and logs to determine the answers to the following kinds of questions:

- Which computers are infected?
- Which computers need scanning?
- What risks were detected in the network?

Table 170: Tasks for monitoring endpoint protection

Task	Description
Review the security status of your network	The following list describes some of the tasks that you can perform to monitor the security status of your client computers. • View the number of clients that did not get installed. See: Running a report on the deployment status of clients • View the number of computers that are offline. See: Finding offline computers • Obtain a count of detected viruses and other security risks and view details for each virus and security risk. See: Viewing risks • Obtain a count of unprotected computers in your network and view the details for each computer. See: Viewing system protection • View the number of computers with up-to-date virus and spyware definitions. See: Viewing system protection • View the real-time operational status of your client computers. See: Viewing the protection status of client computers • Review the processes that run in your network. See: Monitoring SONAR detection results to check for false positives • Locate which computers are assigned to which groups. • View a list of the Symantec Endpoint Protection software versions that are installed on the clients and Symantec Endpoint Protection Manager servers in your network. See: Generating a list of the Symantec Endpoint Protection versions installed in your network • View the licensing information on the client computers, which includes the number of valid seats, over-deployed seats, expired seats, and expiration date. See: Checking the license status in Symantec Endpoint Protection Manager For more information, see: • Viewing a daily or weekly status report • Home page
Locate which client computers need protection	You can perform the following tasks to view or find which computers need additional protection: • View the number of computers with Symantec Endpoint Protection disabled. See: Viewing system protection • View the number of computers with out-of-date virus and spyware definitions. See: Viewing system protection • Find the computers that have not been scanned recently. See: Finding unscanned computers • View attack targets and sources. See: Viewing attack targets and sources • View event logs. See: Viewing logs
Protect your client computers	You can run commands from the console to protect the client computers. See: Running commands on client computers from the console For example, you can eliminate security risks on client computers. See: Checking the scan action and rescanning the identified computers

Task	Description
Configure notifications to alert you when security events occur	You can create and configure notifications to be triggered when certain security-related events occur. For example, you can set a notification to occur when an intrusion attempt occurs on a client computer. See: Setting up administrator notifications
Create custom quick reports and scheduled reports for ongoing monitoring	You can create and generate customized quick reports and you can schedule custom reports to run regularly with the information that you want to see. See: • Running and customizing quick reports • How to run scheduled reports • Saving custom reports • Configuring reporting preferences
Minimize the amount of space that client logs take	For security purposes, you might need to retain log records for a longer period of time. However, if you have a large number of clients, you may have a large volume of client log data. If your management server runs low on space, you might need to decrease the log sizes, and the amount of time the database keeps the logs. You can reduce the volume of log data by performing the following tasks: • Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. See: Specifying client log size and which logs to upload to the management server • Specify how many log entries the client computer can keep in the database, and how long to keep them. See: Specifying the log size and how long to keep log entries in the database • Filter the less important risk events and system events out so that less data is forwarded to the server. See: Modifying log handling and notification settings on Windows computers • Reduce the number of clients that each management server manages. • Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See: Updating policies and content on the client using push mode or pull mode • Reduce the amount of space in the directory where the log data is stored before being inserted into the database. See: About increasing the disk space on the server for client log data
Export log data to a centralized location	Log data export is useful if you want to accumulate all logs from your entire network in a centralized location. Log data export is also useful if you want to use a third-party program such as a spreadsheet to organize or manipulate the data. You also might want to export the data in your logs before you delete log records. You can export the data in some logs to a comma-delimited text file. You can export other logs' data to a tab-delimited text file that is called a dump file or to a Syslog server. See: • Exporting log data to a text file • Exporting data to a Syslog server • Viewing logs from other sites
Troubleshoot issues with reports and logs	You can troubleshoot some issues with reporting. See: Troubleshooting reporting issues

NOTE

Symantec Endpoint Protection pulls the events that appear in the reports from the event logs on your management servers. The event logs contain time-stamps in the client computers' time zones. When the management server receives the events, it converts the event time-stamps to Greenwich Mean Time (GMT) for insertion into the database. When you create reports, the reporting software displays information about events in the local time of the computer on which you view the reports.

Finding unscanned computers

You can list the computers that need scanning. See:

[Monitoring the Symantec Endpoint Protection clients](#)

To find unscanned computers

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, specify the following information:

Report type	You select Scan .
Selected report	You select Computers Not Scanned .

3. Click **Create Report**.

Finding offline computers

You can list the computers that are offline.

A client may be offline for a number of reasons. You can identify the computers that are offline and remediate these problems in a number of ways. See:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

To find offline computers

1. In the console, click **Home**.
2. On the **Home** page, in the **Endpoint Status** pane, click the link that represents the number of offline computers.
3. To get more information about offline computers, click the **View Details** link.

To view offline client computers in the Computer Status log

1. In the console, click **Monitors**.
2. On the **Logs** tab, from the **Log type** list box, click **Computer Status**.
3. Click **Additional Settings**.
4. In the Online status list box, click **Offline**.
5. Click **View Log**.

By default, a list of the computers that have been offline for the past 24 hours appears. The list includes each computer's name, IP address, and the last time that it checked in with its server. You can adjust the time range to display offline computers for any time range you want to see.

Generating a list of the Symantec Endpoint Protection versions installed in your network

You can run a quick report from Symantec Endpoint Protection Manager that provides a list of the Symantec Endpoint Protection software versions that are installed in your network. This list can be useful when you want to upgrade or migrate your software from a previous version of Symantec Endpoint Protection. The list includes local and remote computers.

You can save the report using MHTML webpage archive format. See:

[Printing and saving a copy of a report](#)

To generate a report that lists the Symantec Endpoint Protection software versions

1. In the console, click **Reports**.

-
2. For **Report type**, select **Computer Status**.
 3. For **Select a report**, select **Symantec Endpoint Protection Product Versions**.
 4. Click **Create Report**.

To generate a detailed list of client computers, including Symantec Endpoint Protection software versions

1. In the console, click **Monitors**, and then click the **Logs** tab.
2. For **Log type**, select **Computer Status**.
3. Adjust the **Time range** if desired, and then click **View log**.
4. Scroll to find the column **Version**. Click on the header to sort by version number.
Click **View Applied Filters** to adjust the log filters. Click **Export** to export the list. Click a client computer and then click **Details** to see its details.

More information

- [Viewing logs](#)
- [Choosing which method to upgrade the client software](#)
- [Upgrade resources for Symantec Endpoint Protection](#)

Running a report on the deployment status of clients

You can run several reports on the deployment status of your clients. For example, you can see how many clients were successfully or unsuccessfully installed. You can also see which clients have which protection technologies installed on them, along with system information about the client computers. See:

[Monitoring the Symantec Endpoint Protection clients](#)

To view the status of deployed clients

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, click the **Computer Status** report type, and then click one of the following reports:
 - For the deployment status of the clients, click **Deployment Report**.
 - For the protection status of the clients, click **Client Inventory Details**.
3. Click **Create Report**.

Viewing risks

Generate reports to get information about risks in your network.

[Monitoring the Symantec Endpoint Protection clients](#)

To view risks

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, click the **Report type** drop-down list and select **Risk**.

3. Click the **Selected report** drop-down list, and select the report for the type of risks that you want to view. Some suggestions are as follows:

Risk type	Selected report option
Infected endpoints and endpoints that are at risk	Infected and at-risk computers
Better understand the benefits and risks of not enabling certain features. This report provides the following information: • Signature-based detections of virus and spyware • SONAR (Behavioral Analysis) detections • Download Insight detections • Intrusion Prevention and browser protection detections	Risk Distribution by Protection Technology
Newly detected risks	New Risks Detected in the Network
Comprehensive risk report, which includes multiple reports about risks detected over time.	Comprehensive Risk Report

4. Click **Create Report**.

Viewing attack targets and sources

Generate reports to get information about attack targets and their sources.

To view attack targets and sources

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, click the **Report type** drop-down list and select **Network and Host Exploit Mitigation**.
3. Click the **Select a report** drop-down list and select the report that you want to generate. Some suggestions are as follows:
 - **Top Targets Attacked**
 - **Top Sources of Attack**
 - **Full Report**
 - You can click **Generate** to select the details that you want to appear in the Full Report.
4. Click **Create Report**.

[Monitoring the Symantec Endpoint Protection clients](#)

Viewing Symantec Endpoint Protection reports

Stay informed about what is occurring with Symantec Endpoint Protection by viewing daily or weekly status reports.

The Daily Status Report provides the following information:

- Virus detection counts for cleaned, suspicious, blocked, quarantined, deleted, newly infected, and still infected actions.
- Virus definition distribution timeline
- Top 10 risks and infections

The Weekly Status Report provides the following information:

- Computer status
- Virus detection
- Protection status snapshot
- Virus definition distribution timeline
- Risk distribution by day
- Top 10 risks and infections

For more information, see:

Monitoring the Symantec Endpoint Protection clients

To view a daily status report

1. In the console, click **Home**.
2. On the **Home** page, in the **Favorite Reports** pane, click **Symantec Endpoint Protection Daily Status** or **Symantec Endpoint Protection Weekly Status**.

Viewing system protection

System protection comprises the following information:

- The number of computers with up-to-date virus definitions.
- The number of computers with out-of-date virus definitions.
- The number of computers that are offline.
- The number of computers that are disabled.

For more information, see:

Monitoring the Symantec Endpoint Protection clients

To view system protection

1. In the console, click **Home**.
System protection is shown in the **Endpoint Status** pane.
2. In the **Endpoint Status** pane, click **View Details** to view more system protection information.

Configuring reporting preferences

You can configure the following reporting preferences:

- The **Home** and **Monitors** pages display options
- The **Security Status** thresholds
- The display options that are used for the logs and the reports, as well as legacy log file uploading

The security status thresholds that you set determine when the Security Status message on the Symantec Endpoint Protection Manager **Home** page is considered Poor. Thresholds are expressed as a percentage and reflect when your network is considered to be out of compliance with your security policies.

For example, you can set the percentage of computers with out-of-date virus definitions that triggers a poor security status. You can also set how many days old the definitions need to be to qualify as out of date. Symantec Endpoint Protection determines what is current when it calculates whether signatures or definitions are out of date as follows. Its standard is the most current virus definitions and IPS signature dates that are available on the management server on which the console runs.

For information about the preference options that you can set, you can click **Help** on each tab in the **Preferences** dialog box.

To configure reporting preferences

1. In the console, on the **Home** page, click **Preferences**.
2. Click one of the following tabs, depending on the type of preferences that you want to set:
 - **Home and Monitors**
For more information, see:
[Preferences: Home page and Monitors page](#)
 - **Security Status**
For more information, see:

[Preferences: Security Status](#)

- **Logs and Reports**

For more information, see:

[Preferences: Logs and Reports](#)

3. Set the values for the options that you want to change.

4. Click **OK**.

Logging on to reporting from a standalone web browser

You can access the **Home**, **Monitors**, and **Reports** pages from a standalone web browser that is connected to your management server. However, all of the other console functions are not available when you use a standalone browser.

Report pages and log pages always display in the language that the management server was installed with. To display these pages when you use a remote console or browser, you must have the appropriate font installed on the computer that you use.

To access reporting from a web browser, you must have the following information:

- The host name of the management server.
- Your user name and password for the management server.

NOTE

Check the system requirements for the minimum browser version that is supported with the Symantec Endpoint Protection version in use. Earlier web browser versions are not supported. See:

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

To log on to reporting from a standalone web browser

1. Open a web browser.
2. Type the default reporting URL into the address text box in the following format:

`https://SEPMServer:8445/reporting`

Where SEPMServer is the host name or IP address of the management server.

For a list of supported web browsers, see:

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets. For example: `https://[SEPMServer]:8445`

IPv6 is supported as of version 14.2.

NOTE

When you enter the HTTPS standalone reporting URL in your browser, the browser might display a warning. The warning appears because the certificate that the management server uses is self-signed. To work around this issue, you can install the certificate in your browser's trusted certificate store. The certificate supports host names only, so use the host name in the URL. If you use localhost, IP address, or the fully qualified domain name, a warning still appears.

3. When the logon dialog box appears, type your user name and password, and then click **Log On**.

If you have more than one domain, in the **Domain** text box, type your domain name.

About the types of Symantec Endpoint Protection Manager reports

The following categories of reports are available:

- Quick reports, which you run on demand.
- Scheduled reports, which run automatically based on a schedule that you configure.

Reports include the event data that is collected from your management servers as well as from the client computers that communicate with those servers. You can customize reports to provide the information that you want to see.

The quick reports are predefined, but you can customize them and save the filters that you used to create the customized reports. You can use the custom filters to create custom scheduled reports. When you schedule a report to run, you can configure it to be emailed to one or more recipients.

A scheduled report always runs by default. You can change the settings for any scheduled report that has not yet run. You can also delete a single scheduled report or all of the scheduled reports.

Table 171: Report types available as quick reports and scheduled reports

Report type	Description
Audit	Displays the information about the policies that clients and locations use currently. It includes information about policy modification activities, such as the event times and types, policy modifications, domains, sites, administrators, and descriptions. See: Audit log and quick reports
Application and Device Control	Displays the information about events where some type of behavior was blocked. These reports include information about application security alerts, blocked targets, and blocked devices. Blocked targets can be Windows registry keys, DLLs, files, and processes. See: Application and Device Control logs and quick reports
Compliance	Displays the information about how many clients passed or failed the Host Integrity check.
Computer Status	Displays the information about the operational status of the computers in your network, such as which computers have security features turned off. These reports include information about versions, the clients that have not checked in to the server, client inventory, and online status. See: Computer Status logs and reports
Network and Host Exploit Mitigation	Displays the information about intrusion prevention, attacks on the firewall, firewall traffic and packets, and Memory Exploit Mitigation. The Network and Host Exploit Mitigation reports let you track a computer's activity and its interaction with other computers and networks. They record information about the traffic that tries to enter or exit the computers through their network connections. Memory Exploit Mitigation events list which mitigation techniques terminated an application or blocked an exploit from attacking an application. See: Network and Host Exploit Mitigation logs and quick reports
Risk	Displays the information about risk events on your management servers and their clients. It includes information about behavioral analysis (SONAR) scans. See: • Risk logs and quick reports • SONAR logs
Scan	Displays the information about virus and spyware scan activity. See: Scan logs and quick reports
System	Displays the information about event times, event types, sites, domains, servers, and severity levels. The System reports contain information that is useful for troubleshooting client problems. See: System logs and quick reports

If you have multiple domains in your network, many reports let you view data for all domains, one site, or a few sites. The default for all quick reports is to show all domains, groups, servers, and so on, as appropriate for the report you select to create. See:

- [Running and customizing quick reports](#)
- [How to run scheduled reports](#)

The following section describes the reports by name and their general content. You can configure Basic Settings and Advanced Settings for all reports to refine the data you want to view. You can also save your custom filter with a name to run the same custom report at a later time.

Table 172: Audit reports

Report name	Description
Policies Used	This report displays the policies that clients and locations use currently. Information includes the domain name, group name, and the serial number of the policy that is applied to each group.

Table 173: Application and Device Control reports

Report name	Description
Top Groups With Most Alerted Application Control Logs	This report consists of a pie chart with the relative bars. It shows the groups with the application control logs that have generated the largest number of security alerts.
Top Targets Blocked	This report consists of a pie chart with the following targets, if applicable: • Top Files • Top Registry Keys • Top Processes • Top Modules (dlls)
Top Devices Blocked	This report consists of a pie chart that shows the devices most frequently blocked from access to your network.

Table 174: Compliance reports

Report name	Description
Host Integrity Status	This report displays the clients that have passed or failed the Host Integrity check that runs on their computer.
Clients by Compliance Failure Summary	This report consists a bar chart that shows: • A count of the unique workstations by the type of control failure event, such as antivirus, firewall, or VPN • The total number of clients in the group
Compliance Failure Details	This report consists of a table that displays unique computers by control failure. It shows the criteria and the rule that is involved in each failure, along with the percentage of clients that are deployed and the percentage that failed.
Non-compliant Clients by Location	This report consists of a table that shows the compliance failure events. These events display in groups that are based on their location. Information includes the unique computers that failed, and the percentage of total failures and location failures.

Table 175: Computer Status reports

Report name	Description
Virus Definition Distributions	This report displays the unique virus definitions file versions that are used throughout your network and the number of computers and percentage using each version.
Computers Not Recently Updated	This report displays a list of all the computers that have not been recently updated. It also displays the computer's operating system, IP address, user name, and the last time its status was changed.
Symantec Endpoint Protection Product Versions	This report displays the list of version numbers for all the Symantec Endpoint Protection product versions in your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
Intrusion Prevention Signature Distribution	This report displays the IPS signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
Download Protection Signature Distribution	This report displays the download protection signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
SONAR Signature Distribution	This report displays the SONAR signature file versions that are used throughout your network. It also includes the domain and server for each, as well as the number of computers and percentage of each.
Client Inventory	This report consists of a bar chart that displays the total number of computers and percentages of: • Operating System • Total Memory • Free Memory • Total Disk Space • Free Disk Space • Processor Type
Compliance Status Distribution	This report consists of a pie chart with relative bars that show compliance passes and failures by group or by subnet. It shows the number of computers and the percentage of computers that are in compliance.
Client Online Status	This report consists of pie charts with the relative bars per group or per subnet. It displays the percentage of your computers that are online. Online has the following meanings: • For the clients that are in push mode, online means that the clients are currently connected to the server • For the clients that are in pull mode, online means that the clients have contacted the server within the last two client heartbeats • For the clients in remote sites, online means that the clients were online at the time of the last replication
Clients With Latest Policy	This report consists of pie charts per group or subnet. It displays the number of computers and percentage that have the latest policy applied.
Client Count by Group	This report consists of a table that lists host information by group. It displays the number of clients and users. If you use multiple domains, this information appears by domain.
Security Status Summary	This report reflects the general security status of the network, and displays the number and percentage of computers that have the following status: • The Antivirus English is off • Auto-protect is off • Tamper Protection is off • Restart is required • A Host Integrity check failed • Network Threat Protection is off

Report name	Description
Protection Content Versions	This report displays all the proactive protection content versions that are used throughout your network. One pie chart is displayed for each of the following types of protection: • Decomposer versions • Eraser Engine versions • SONAR Content versions • SONAR Engine versions • Commercial Application List versions • Content Handler Engine versions • Permitted Application List versions • The new content types that Symantec Security Response has added
Symantec Endpoint Protection Licensing Status	This report contains days remaining for trial license expiration and instructions to add new licenses.
Client Inventory Details	This report contains details of client inventory, such as computer specifications and signatures.
Client Software Rollout (Snapshots) Scheduled report only	This report consists of tables that track the progression of client package deployments. The snapshot information lets you see how quickly the rollout progresses, and how many clients are still not fully deployed.
Clients Online/Offline Over Time (Snapshots) Scheduled report only	This report consists of line charts and tables that shows the number of clients online or offline. One chart displays for each of the top targets. The target is either a group or an operating system.
Clients With Latest Policy Over Time (Snapshots) Scheduled report only	This report consists of a line chart that displays the clients that have the latest policy applied. One chart displays for each of the top clients.
Non-Compliant Clients Over Time (Snapshots) Scheduled report only	This report consists of a line chart that shows the percentage of clients that have failed a host integrity check over time. One chart displays for each of the top clients.
Virus Definition Rollout (Snapshots) Scheduled report only	This report lists the virus definitions package versions that have been rolled out to clients. This information is useful for tracking the progress of deploying new virus definitions from the console.
Deployment Report	This report summarizes the state of client installations and deployments.

Table 176: Network and Host Exploit Mitigation reports

Report name	Description
Top Targets Attacked	Includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks. You can view information using groups, subnets, clients, or ports as the target.
Top Sources of Attack	Shows the top hosts that initiated attacks against your network. It includes information such as the number and percentage of attacks, the attack type and severity, and the distribution of attacks.
Top Types of Attack	Includes information such as the number and percentage of events, the group and severity, and the event type and number by group.
Top Blocked Applications	Shows the top applications that were prevented from accessing your network. It includes information such as the number and percentage of attacks, the group and severity, and the event type and number by group.
Attacks Over Time	Shows the attacks during the selected time period. For example, if the time range is the last month, the report displays the total number of attacks per day for the past month. It includes the number and percentage of attacks. You can view attacks for all computers, or by the top operating systems, users, IP addresses, groups, or attack types.

Report name	Description
Security Events by Severity	Displays the total number and percentage of security events in your network, ranked according to their severity.
Blocked Applications Over Time	Displays the total number of applications that were prevented from accessing your network over a time period that you select. It includes the event time, the number of attacks, and the percentage. You can display the information for all computers, or by group, IP address, operating system, or user.
Traffic Notifications Over Time	Shows the number of notifications that were based on firewall rule violations over time. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can display the information in this report for all computers, or by group, IP address, operating system, or user.
Top Traffic Notifications	Lists the group or subnet, and the number and percentage of notifications. It shows the number of notifications that were based on firewall rule violations that you configured as important to be notified about. The rules that are counted are those where you checked the Send Email Alert option in the Logging column of the Firewall Policy Rules list. You can view information for all, for the Traffic log, or for the Packet log, grouped by top groups or subnets.
Memory Exploit Mitigation Detections	Displays the number of memory exploit mitigation types that have been blocked or allowed.
Top URL Detections	Lists the URLs that URL reputation blocks.
Full Report	Lists the top Network Threat Protection items in a single report.

Table 177: Risk reports

Report name	Description
Infected and At Risk Computers	This report consists of two tables. One table lists computers that have a virus infection, and the other table lists the computers that have a security risk that has not yet been remediated.
Action List	This report consists of a table that shows a count of all the possible actions that were taken when risks were detected. The possible actions are Cleaned, Suspicious, Blocked, Quarantined, Deleted, Pending Repair, Logged Commercial or Forced detections, Newly Infected, and Still Infected. This information also appears on the Symantec Endpoint Protection Home page.
Risk Detections Count	This report consists of a pie chart, a risk table, and an associated relative bar. It shows the number of risk detections by domain, server, or computer. If you have legacy Symantec AntiVirus clients, the report uses the server group rather than the domain.
New Risks Detected in the Network	This report consists of a table and a distribution pie chart. For each new risk, the table provides the following information: • Risk name • Risk category or type • First discovered data • First occurrence in the organization • Scan type that first detected it • Domain where it was discovered (server group on legacy computers) • Server where it was discovered (parent server on legacy computers) • Group where it was discovered (parent server on legacy computers) • The computer where it was discovered and the name of the user that was logged on at the time The pie chart shows new risk distribution by the target selection type: domain (server group on legacy computers), group, server (parent server on legacy computers), computer, or user name.

Report name	Description
Top Risk Detection Correlation	This report consists of a three-dimensional bar graph that correlates virus and security risk detections by using two variables. You can select from computer, user name, domain, group, server, or risk name for the x and y axis variables. This report shows the top five instances for each axis variable. If you selected computer as one of the variables and there are fewer than five infected computers, non-infected computers may appear in the graph. Note: For computers running legacy versions of Symantec AntiVirus, the server group and parent server are used instead of domain and server.
Download Risk Distribution	This report displays the number of files detected by Download Insight and groups them by sensitivity level. Detailed reports are given to files that have been found. You can also group files by URL, web domain, application, and user-allowed before running the report.
Risk Distribution Summary	This report consists of a pie chart and an associated bar graph that displays a relative percentage for each unique item from the chosen target type. For example, if the chosen target is risk name, the pie chart displays slices for each unique risk. A bar is shown for each risk name and the details include the number of detections and its percentage of the total detections.
Risk Distribution Over Time	This report consists of a table that displays the number of virus and security risk detections per unit of time and a relative bar.
Risk Distribution by Protection Technology	This report displays the number of virus and security risk detections per protection technology.
SONAR Detection Results	This report consists of a pie chart and bar graphs that display the following information: • A list of the applications that are labeled as risks that you have added to your exceptions as permitted in your network • A list of the applications that have been detected that are confirmed risks • A list of the applications that have been detected but whose status as a risk is still unconfirmed For each list, this report displays the company name, the application hash and the version, and the computer involved. For the permitted applications, it also displays the source of the permission.
SONAR Threat Distribution	Displays the top application names that have been detected with relative bars and a summary table. The detections include applications on the Commercial Applications List and Forced Detections lists. The first summary table contains the application name and the number and percentage of detections.
SONAR Threat Detection Over Time	This report consists of a line chart that displays the number of proactive threat detections for the time period selected. It also contains a table with relative bars that lists the total numbers of the threats that were detected over time.
Action Summary for Top Risks	This report lists the top risks that have been found in your network. For each, it displays action summary bars that show the percentage of each action that was taken when a risk was detected. Actions include quarantined, cleaned, deleted, and so on. This report also shows the percentage of time that each particular action was the first configured action, the second configured action, neither, or unknown.
Number of Notifications	This report consists of a pie chart with an associated relative bar. The charts show the number of notifications that were triggered by the firewall rule violations that you have configured as important to be notified about. It includes the type of notifications and the number of each.
Number of Notifications Over Time	This report consists of a line chart that displays the number of notifications in the network for the time period selected. It also contains a table that lists the number of notifications and percentage over time. You can filter the data to display by the type of notification, acknowledgment status, creator, and notification name.
Weekly Outbreaks	This report displays the number of virus and security risk detections and a relative bar per week for each for the specified time range. A range of one day displays the past week.
Comprehensive Risk Report	This report, by default, includes all of the distribution reports and the new risks report. However, you can configure it to include only certain reports. This report includes the information for all domains.
Symantec Endpoint Protection Daily Status	This report contains virus detection, intervention and definition status for network events over the previous 24 hours.

Report name	Description
Symantec Endpoint Protection Weekly Status	This report contains licensing status and virus detection statistics for endpoint computers over the previous week. Data reflects cumulative values unless otherwise noted.

Table 178: Scan reports

Report name	Description
Scan Statistics Histogram	This report consists of a histogram where you can select how you want the following information in the scan to be distributed: • By the scan time (in seconds) • By the number of risks detected • By the number of files with detections • By the number of files that are scanned • By the number of files that are omitted from scans You can also configure the bin width and how many bins are used in the histogram. The bin width is the data interval that is used for the group by selection. The number of bins specifies how many times the data interval is repeated in the histogram. The information that displays includes the number of entries and the minimum and the maximum values, as well as the average and the standard deviation. You might want to change the report values to maximize the information that is generated in the report's histogram. For example, you might want to consider the size of your network and the amount of information that you view.
Computers by Last Scan Time	This report shows a list of computers in your security network by the last time scanned. It also includes the IP address and the name of the user that was logged in at the time of the scan.
Computers Not Scanned	This report shows a list of computers in your security network that have not been scanned and provides the following formation: • The IP address • The time of the last scan • The name of the current user or the user that was logged on at the time of the last scan

Table 179: System reports

Report name	Description
Top Clients that Generate Errors	This report consists of a pie chart for each warning condition and error condition. The charts show the relative error count and relative warning count and percentage, by client.
Top Servers that Generate Errors	This report consists of a pie chart for each warning condition and error condition. The chart shows the relative error count and relative warning count and percentage, by server.
Database Replication Failures Over Time	This report consists of a line chart with an associated table that lists the replication failures for the time range selected.
Site Status Report	This report shows a real-time summary of the health status of all sites and information on all servers on the local site.
Network Integration Token Usage	This report summarizes the usage of the integration token for client authentication with Web and Cloud Access Protection.

Running and customizing quick reports

Quick reports are predefined, customizable reports. These reports include event data collected from your management servers as well as the client computers that communicate with those servers. Quick reports provide information on events

specific to the settings you configure for the report. You can save the report settings so that you can run the same report at a later date, and you can print and save reports.

Quick reports are static; they provide information specific to the time frame you specify for the report. Alternately, you can monitor events in real time using the logs.

To run a quick report

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, in the **Report type** list box, select the type of report that you want to run.
3. In the **Select a report** list box, select the name of the report you want to run.
4. Click **Create Report**.

To customize a quick report

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, in the **Report type** list box, select the type of report that you want to customize.
3. In the **Select a report** list box, select the name of the report you want to customize.
 - For the **Network Compliance Status** report and the **Compliance Status** report, in the **Status** list box, select a saved filter configuration that you want to use, or leave the default filter.
 - For the **Top Risk Detections Correlation** report, you can select values for the **X-axis** and **Y-axis** list boxes to specify how you want to view the report.
 - For the **Scan Statistics Histogram Scan** report, you can select values for **Bin width** and **Number of bins**.
 - For some reports, you can specify how to group the report results in the **Group** list box. For other reports, you can select a target in the **Target** field on which to filter report results.
4. In the **Use a saved filter** list box, select a saved filter configuration that you want to use, or leave the default filter.
5. Under **What filter settings would you like to use?**, in the **Time range** list box, select the time range for the report.
6. If you select **Set specific dates**, then use the **Start date** and **End date** list boxes. These options set the time interval that you want to view information about.

When you generate a Computer Status report and select **Set specific dates**, you specify that you want to see all entries that involve a computer that has not checked in with its server since the time you specify in the date and time fields.

7. If you want to configure additional settings for the report, click **Additional Settings** and set the options that you want. You can click **Tell me more** to see descriptions of the filter options in the context-sensitive help.

NOTE

The filter option text boxes that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

You can save the report configuration settings if you think you will want to run this report again in the future.

8. Click **Create Report**.

More information

- [Saving custom reports](#)
- [Printing and saving a copy of a report](#)
- [How to run scheduled reports](#)

Saving custom reports

You can save custom report settings in a filter so that you can generate the report again at a later date. When you save your settings, they are saved in the database. The name that you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

NOTE

The filter configuration settings that you save are available for your user logon account only. Other users with reporting privileges do not have access to your saved settings.

For more information, see:

[Editing the filter used for a scheduled report](#)

You can delete any report configuration that you create. When you delete a configuration, the report is no longer available. The default report configuration name appears in the **Use a saved report** list box and the screen is repopulated with the default configuration settings.

NOTE

If you delete an administrator from the management server, you have the option to save the reports that were created by the deleted administrator. The ownership of the reports is changed, and the report names are changed. The new report name is in the format `"OriginalName('AdminName')"`. For example, a report that was created by administrator JSmith, named `Monday_risk_reports`, would be renamed `Monday_risk_reports(JSmith)`.

For more information, see:

[About administrator accounts and access rights](#)

To save a custom report

1. In the console, click **Reports**.
2. On the **Quick Reports** tab, select a report type from the list box.
3. Change any basic settings or additional settings for the report.
4. Click **Save Filter**.
5. In the **Filter name** text box, type a descriptive name for this report filter. Only the first 32 characters of the name that you give display when the filter is added to the **Use a saved filter** list.
6. Click **OK**.
7. When the confirmation dialog box appears, click **OK**.

After you save a filter, it appears in the **Use a saved filter** list box for related reports and logs.

How to run scheduled reports

Scheduled reports are the reports that run automatically based on the schedule that you configure. Scheduled reports are emailed to recipients, so you must include the email address of at least one recipient. After a report runs, the report is emailed to the recipients that you configure as an .mht file attachment.

The data that appears in the scheduled reports is updated in the database every hour. At the time that the management server emails a scheduled report, the data in the report is current to within one hour.

The other reports that contain data over time are updated in the database based on the upload interval that you configured for the client logs. See:

[Specifying client log size and which logs to upload to the management server](#)

NOTE

If you have multiple servers within a site that share a database, only the first-installed server runs the reports scheduled for the site. This default ensures that all the servers in the site do not run the same scheduled scans simultaneously. If you want to designate a different server to run scheduled reports, you can configure this option in the local site properties.

To run scheduled reports

1. In the console, click **Reports**.
2. On the **Scheduled Reports** tab, click **Add**.
3. In the **Report name** text box, type a descriptive name and optionally, type a longer description.
Although you can paste more than 255 characters into the description text box, only 255 characters are saved in the description.
4. If you do not want this report to run until another time, uncheck the **Enable this scheduled report** check box.
5. Select the report type that you want to schedule from the list box.
6. Select the name of the specific report that you want to schedule from the list box.
7. Select the name of the saved filter that you want to use from the list box.
8. In the **Run every** text box, select the time interval at which you want the report to be emailed to recipients (hours, days, weeks, months). Then, type the value for the time interval you selected. For example, if you want the report to be sent to you every other day, select days and then type 2.
9. In the **Start after** text box, type the date that you want the report to start or click the calendar icon and select the date. Then, select the hour and minute from the list boxes.
10. Under **Report Recipients**, type one or more comma-separated email addresses.
You must already have set up mail server properties for email notifications to work.
11. Click **OK**.

Editing the filter used for a scheduled report

You can change the settings for any report that you have already scheduled. The next time the report runs it uses the new filter settings. You can also create additional scheduled reports, which you can base on a previously saved report filter.

Filter storage is based in part on the creator, so problems do not occur when two different users create a filter with the same name. However, an individual user or two users who log on to the default admin account should not create filters with the same name.

If users create filters with the same name, a conflict can occur under two conditions:

- Two users are logged on to the default admin account on different sites and each creates a filter with the same name.
- One user creates a filter, logs on to a different site, and immediately creates a filter with the same name.

If either condition occurs before site replication takes place, the user subsequently sees two filters with the same name in the filter list. Only one of the filters is usable. If this problem occurs, it is a best practice to delete the usable filter and recreate it with a different name. When you delete the usable filter, you also delete the unusable filter.

For more information, see:

[Saving custom reports](#)

NOTE

When you associate a saved filter with a scheduled report, make sure that the filter does not contain custom dates. If the filter specifies a custom date, you get the same report every time the report runs.

For more information, see:

[How to run scheduled reports](#)

To edit the filter used for a scheduled report

-
1. In the console, click **Reports**.
 2. Click **Scheduled Reports**.
 3. In the list of reports, click the scheduled report that you want to edit.
 4. Click **Edit Filter**.
 5. Make the filter changes that you want.
 6. Click **Save Filter**.
If you want to retain the original report filter, give this edited filter a new name.
 7. Click **OK**.
 8. When the confirmation dialog box appears, click **OK**.

Printing and saving a copy of a report

You can print a report or save a copy of a Quick Report. You cannot print scheduled reports. A saved file or printed report provides a snapshot of the current data in your reporting database so that you can retain a historical record.

NOTE

By default, Internet Explorer does not print background colors and images. If this printing option is disabled, the printed report may look different from the report that you created. You can change the settings in your browser to print background colors and images.

For more information, see:

[Running and customizing quick reports](#)

When you save a report, you save a snapshot of your security environment that is based on the current data in your reporting database. If you run the same report later, based on the same filter configuration, the new report shows different data.

To print a copy of a report

1. In the report window, click **Print**.
2. In the **Print** dialog box, select the printer you want, if necessary, and then click **Print**.

To save a copy of a report

1. In the report window, click **Save**.
2. In the **File Download** dialog box, click **Save**.
3. In the **Save As** dialog box, in the **Save in selection** dialog box, browse to the location where you want to save the file.
4. In the **File name** list box, change the default file name, if desired.
5. Click **Save**.
The report is saved in MHTML Web page archive format in the location you selected.
6. In the **Download complete** dialog box, click **Close**.

Viewing logs

You can generate a list of events to view from your logs that are based on a collection of filter settings that you select.

NOTE

If database errors occur when you view the logs that include a large amount of data, you might want to change the database timeout parameters.

If you get CGI or terminated process errors, you might want to change other timeout parameters.

For more information, see:

[Changing timeout parameters for reviewing reports and logs](#)

Reports and logs always appear in the language that the management server was installed with. To display these when you use a remote Symantec Endpoint Protection Manager console or browser, you must have the appropriate font installed on the computer that you use. See:

- [About the types of Symantec Endpoint Protection Manager logs](#)
- [Saving and deleting custom logs by using filters](#)

To view logs

1. In the console, click **Monitors**.
2. On the **Logs** tab, from the **Log type** list box, select the type of log that you want to view.
3. For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to view.
4. In the **Use a saved filter** list box, select a saved filter or leave the value **Default**.
5. Select a time from the **Time range** list box or leave the default value. If you select **Set specific dates**, then set the date or dates and time from which you want to display entries.
6. Click **Additional Settings** to limit the number of entries you display.

You can also set any other available **Additional Settings** for the type of log that you selected.

NOTE

The filter option fields that accept wildcard characters and search for matches are not case-sensitive. The ASCII asterisk character is the only asterisk character that can be used as a wildcard character.

7. Click **View Log**.

You can also click **Save Filter** to save the filter configuration to generate the same log view at a later date.

About the types of Symantec Endpoint Protection Manager logs

Logs contain records about client configuration changes, security-related activities, and errors. These records are called *events*. The logs display these events with any relevant additional information. Security-related activities include information about virus detections, computer status, and the traffic that enters or exits the client computer.

Logs are an important method for tracking each client computer's activity and its interaction with other computers and networks. You can use this data to analyze the overall security status of the network and modify the protection on the client computers. You can track the trends that relate to viruses, security risks, and attacks. If several people use the same computer, you might be able to identify who introduces risks, and help that person to use better precautions.

You can view the log data on the **Logs** tab of the **Monitors** page.

The management server regularly uploads the information in the logs from the clients to the management server. You can view this information in the logs or in reports. Because reports are static and do not include as much detail as the logs, you might prefer to monitor the network by using logs.

In addition to using the logs to monitor your network, you can take the following actions from various logs:

- Run commands on client computers. See:
[Running commands on client computers from the console](#)
- Add several kinds of exceptions. See:
[Creating exceptions from log events](#)
- Delete files from the **Quarantine**. See:

Managing the quarantine for Windows clients

The following table describes the different types of content that you can view and the actions that you can take from each log.

Table 180: Log types

Log type	Contents and actions
Audit	The Audit log contains information about policy modification activity. Available information includes the event time and type; the policy modified; the domain, site, and user name involved; and a description. No actions are associated with this log. For more information, see: Audit log and quick reports
Application and Device Control	The Application Control log and the Device Control log contain information about events where some type of behavior was blocked. The following Application and Device Control logs are available: • Application Control, which includes information about Tamper Protection • Device Control Available information includes the time the event occurred, the action taken, and the domain and computer that were involved. It also includes the user that was involved, the severity, the rule that was involved, the caller process, and the target. You can create an application control or Tamper Protection exception from the Application Control log. For more information, see: • Creating an application exception • Application and Device Control logs and quick reports
Compliance	The compliance logs contain information about client Host Integrity. No actions are associated with these logs. For more information, see: Compliance log and quick report
Computer Status	The Computer Status log contains information about the real-time operational status of the client computers in the network. Available information includes the computer name, IP address, infected status, protection technologies, Auto-Protect status, versions, and definitions date. It also includes the user, last check-in time, policy, group, domain, and restart required status. You can also clear the infected status of computers from this log. Note: This log contains information that is collected from both Windows clients and Mac clients. For more information, see: Computer Status logs and reports
Network and Host Exploit Mitigation	The Network and Host Exploit Mitigation logs contain information about intrusion prevention, the firewall, and Memory Exploit Mitigation. The logs contain information about attacks on the firewall and on intrusion prevention. Information is available about denial-of-service attacks, port scans, and the changes that were made to executable files. They also contain information about the connections that are made through the firewall (traffic), and the data packets that pass through. These logs also contain some of the operational changes that are made to computers, such as detecting network applications, and configuring software. For more information, see: Network and Host Exploit Mitigation logs and quick reports

Log type	Contents and actions
SONAR	The SONAR log contains information about the threats that have been detected during behavioral analysis (SONAR) threat scans. These are real-time scans that detect potentially malicious applications when they run on your client computers. The information includes items such as the time of occurrence, event actual action, user name, Web domain, application, application type, file, and path. For more information, see: • SONAR logs • What is Behavioral Analysis (SONAR) in Symantec Endpoint Protection?
Risk	The Risk log contains information about risk events. Available information includes the event time, event actual action, user name, computer, and domain, risk name and source, count, and file and path. For more information, see: Risk logs and quick reports
Scan	The Scan log contains information about virus and spyware scan activity from both Windows clients and Mac clients. Available information includes items such as the scan start, computer, IP address, status, duration, detections, scanned, omitted, and domain. No actions are associated with these logs. For more information, see: Scan logs and quick reports
System	The system logs contain information about events such as when services start and stop. No actions are associated with these logs. For more information, see: System logs and quick reports

Saving and deleting custom logs by using filters

You can construct custom filters by using the **Basic Settings** and **Additional Settings** to change the information that you want to see. You can save your filter settings to the database so that you can generate the same view again in the future. When you save your settings, they are saved in the database. The name you give to the filter appears in the **Use a saved filter** list box for that type of logs and reports.

NOTE

If you selected **Past 24 hours** as the time range for a log filter, the 24-hour time range begins when you first select the filter. If you refresh the page, the start of the 24-hour range does not reset. If you select the filter, and wait to view a log, the time range starts when you select the filter. It does not start when you view the log.

If you want to make sure the past 24-hour range starts now, select a different time range and then reselect **Past 24 hours**.

To save a custom log by using a filter

1. In the main window, click **Monitors**.
2. On the **Logs** tab, select the type of log view that you want to configure a filter for from the **Log type** list box.
3. For some types of logs, a **Log content** list box appears. If it appears, select the log content that you want to configure a filter for.
4. In the **Use a saved filter** list box, select the filter that you want to start from. For example, select the default filter.
5. Under **What filter settings would you like to use**, click **Additional Settings**.
6. Change any of the settings.
7. Click **Save Filter**.

-
8. In the dialog box that appears, in the **Filter name** box, type the name that you want to use for this log filter configuration. Only the first 32 characters of the name that you give display when the saved filter is added to the filter list.
 9. Click **OK** and your new filter name is added to the **Use a saved filter** list box.
 10. When the confirmation dialog box appears, click **OK**.

To delete a saved filter

1. In the **Use a saved filter** list box, select the name of the log filter that you want to delete.
2. Beside the **Use a saved filter** list box, click the **Delete** icon.
3. When you are prompted to confirm that you want to delete the filter, click **Yes**.

Viewing logs from other sites

If you want to view the logs from another site, you must log on to a server at the remote site from the Symantec Endpoint Protection Manager console. If you have an account on a server at the remote site, you can log on remotely and view that site's logs.

If you have configured replication partners, you can choose to have all the logs from the replication partners copied to the local partner and vice versa. If you choose to replicate logs, by default you see the information from both your site and the replicated sites when you view any log. If you want to see a single site, you must filter the data to limit it to the location you want to view. If you choose to replicate logs, be sure that you have sufficient disk space for the additional logs on all the replication partners. See:

[How to install a second site for replication](#)

To view the logs from another site

1. Open a web browser.
2. Type the following in the address text box as follows:

```
http://SEPMServer:9090
```

Where SEPMServer is the server name or the IP address.

The IP address can be either IPv4 or IPv6. You must enclose the IPv6 address with square brackets: `http://[SEPMServer]:9090`

The console then downloads. The computer from which you log on must have the Java Runtime Environment (JRE) installed. If it does not, you are prompted to download and install it. Follow the prompts to install the JRE.

3. In the console logon dialog box, type your user name and password.
4. In the **Server** text box, if it does not fill automatically, type the server name or IP address and port number 8443 as follows:

```
http://SEPMServer:8443
```

5. Click **Log On**.

Exporting data to a Syslog server

To increase the space in the database, you can configure the management server to send the log data to a Syslog server.

When you export log data to a Syslog server, you must configure the Syslog server to receive the logs. See:

[Exporting log data to a text file](#)

To export log data to a Syslog server

1. In the console, click **Admin**.
2. Click **Servers**.
3. Click the local site or remote site that you want to export log data from.
4. Click **Configure External Logging**.
5. On the **General** tab, in the **Update Frequency** list box, select how often to send the log data to the file.
6. In the **Primary Logging Server** list box, select the management server to send the logs to.
If you use SQL Server and connect multiple management servers to the database, specify only one server as the primary logging server.
7. Check **Enable Transmission of Logs to a Syslog Server**.
8. Provide the following information:
 - **Syslog Server**
Type the IP address or domain name of the Syslog server that you want to receive the log data.
 - **Destination Port**
Select the protocol to use, and type the destination port that the Syslog server uses to listen for Syslog messages.
 - **Log Facility**
Type the number of the log facility that you want to the Syslog configuration file to use, or use the default. Valid values range from 0 to 23.
9. On the **Log Filter** tab, check which logs to export.
10. Click **OK**.

Exporting log data to a text file

When you export data from the logs to a text file, by default the files are placed in a folder. By default, that folder path is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\dump. Entries are placed in a .tmp file until the records are transferred to the text file.

NOTE

You cannot restore the database by using exported log data.

The following table shows the correspondence of the types of log data to the names of the exported log data files. The log names do not correspond one-to-one to the log names that are used on the **Logs** tab of the **Monitors** page.

Table 181: Log text file names for Symantec Endpoint Protection

Log Data	Text File Name
Server Administration	scm_admin.log
Application and Device Control	agt_behavior.log
Server Client	scm_agent_act.log
Server Policy	scm_policy.log
Server System	scm_system.log
Client Packet	agt_packet.log
Client Proactive Threat	agt_proactive.log
Client Risk	agt_risk.log
Client Scan	agt_scan.log

Log Data	Text File Name
Client Security	agt_security.log
Client System	agt_system.log
Client Traffic	agt_traffic.log

NOTE

When you export to a text file, the number of exported records can differ from the number that you set in the **External Logging** dialog box. This situation arises when you restart the management server. After you restart the management server, the log entry count resets to zero, but there may already be entries in the temporary log files. In this situation, the first *.log file of each type that is generated after the restart contains more entries than the specified value. Any log files that are subsequently exported contain the correct number of entries.

To export log data to a text file

1. In the console, click **Admin**.
2. Click **Servers**.
3. Click the local site or remote site that you want to configure external logging for.
4. Click **Configure External Logging**.
5. On the **General** tab, select how often you want the log data to be sent to the file.
6. In the **Primary Logging Server** list box, select the server that you want to send logs to.
If you use Microsoft SQL with more than one management server connecting to the database, only one server needs to be the Primary Logging Server.
7. Check **Export Logs to a Dump File**.
8. If necessary, check **Limit Dump File Records** and type in the number of entries that you want to send at a time to the text file.
9. On the **Log Filter** tab, select all of the logs that you want to send to text files.
If a log type that you select lets you select the severity level, you must check the severity levels that you want to export.
10. Click **OK**.

Configuring a failover server for external logging

The Symantec Endpoint Protection Manager acts as a primary logging server to forward logs to the syslog server. As of 14.3, you can set up a second management server to act as a failover server for the primary one. If the primary management server goes offline, the second management server takes over and forwards logs to the syslog server. When the primary management server comes back online, it resumes forwarding the logs.

To configure a failover server for external logging

1. In the console, click **Admin > Servers**, select the site, and click **Configure External Logging**.
2. On the **General** tab, in the **Master Logging Server** drop-down list, select the primary management server you want to send the logs to.
If the primary server goes down, the next management server in the list takes over. The management servers are listed in the reporting server priority list on the **Admin > Servers > Edit Site Properties > General** tab.
3. Click **OK**.

More information

[Installing a management server for failover and load balancing](#)

Managing notifications

Notifications alert administrators and computer users about potential security problems.

Some notification types contain default values when you configure them. These guidelines provide reasonable starting points depending on the size of your environment, but they may need to be adjusted. Trial and error may be required to find the right balance between too many and too few notifications for your environment. Set the threshold to an initial limit, then wait for a few days. After a few days, you can adjust the notifications settings.

For virus, security risk, and firewall event detection, suppose that you have fewer than 100 computers in a network. A reasonable starting point in this network is to configure a notification when two risk events are detected within one minute. If you have 100 to 1000 computers, detecting five risk events within one minute may be a more useful starting point.

You manage notifications on the **Monitors** page. You can use the **Home** page to determine the number of unacknowledged notifications that need your attention.

The following table lists the tasks you can perform to manage notifications.

Table 182: Notification management

Task	Description
Learn about notifications	Learn how notifications work. See: How notifications work
Confirm that the email server is configured to enable email notifications	Notifications sent by email require that the Symantec Endpoint Protection Manager and the email server are properly configured. See: Establishing communication between the management server and email servers
Review preconfigured notifications	Review the preconfigured notifications provided by Symantec Endpoint Protection. See: What are the types of notifications and when are they sent?
View unacknowledged notifications	View and respond to unacknowledged notifications. See: Viewing and acknowledging notifications
Configure new notifications	Optionally create notifications to remind you and other administrators about important issues. See: • Setting up administrator notifications • About turning on notifications for remote clients
Create notification filters	Optionally create filters to expand or limit your view of all of the notifications that have been triggered. See: Saving and deleting administrative notification filters

How notifications work

Notifications alert administrators and users about potential security problems. For example, a notification can alert administrators about an expired license or a virus infection.

Events trigger a notification. A new security risk, a hardware change to a client computer, or a trial license expiration can trigger a notification. Actions can then be taken by the system once a notification is triggered. An action might record the notification in a log, or run a batch file or an executable file, or send an email.

NOTE

Email notifications require that communications between the Symantec Endpoint Protection Manager and the email server are properly configured.

You can set a damper period for notifications. The damper period specifies the time that must pass before the notification condition is checked for new data. When a notification condition has a damper period, the notification is only issued on the first occurrence of the trigger condition within that period. For example, suppose that a large-scale virus attack occurs, and that there is a notification condition configured to send an email whenever viruses infect five computers on the network. If

you set a damper period of one hour for that notification condition, the server sends only one notification email each hour during the attack.

NOTE

If you set the **Damper** period to **None** for notifications about critical events, you should make sure that clients can upload critical events immediately. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.

More information

- [Managing notifications](#)
- [Establishing communication between the management server and email servers](#)
- [What are the types of notifications and when are they sent?](#)
- [Setting up administrator notifications](#)
- [Viewing and acknowledging notifications](#)

What are the types of notifications and when are they sent?

Symantec Endpoint Protection Manager provides notifications for administrators. You can customize most of these notifications to meet your particular needs. For example, you can add filters to limit a trigger condition only to specific computers. Or you can set notifications to take specific actions when they are triggered.

By default, some of these notifications are enabled when you install Symantec Endpoint Protection Manager. Notifications that are enabled by default are configured to log to the server and send email to system administrators.

For more information, see:

- [Managing notifications](#)
- [How upgrades from another version affect notification conditions](#)

Table 183: Preconfigured notifications

Notification	Description
Authentication failure	A configurable number of logon failures in a defined period of time triggers the Authentication failure notification. You can set the number of logon failures and the time period within which they must occur to trigger the notification.
Client list changed	This notification triggers when there is a change to the existing client list. This notification condition is enabled by default. Client list changes can include: • The addition of a client • A change in the name of a client • The deletion of a client • A change in the hardware of a client • A change in the Unmanaged Detector status of a client • A client mode change

Notification	Description
Client security alert	This notification triggers upon any of the following security events: • Compliance events • Network and Host Exploit Mitigation events • Traffic events • Packet events • Device control events • Application control events You can modify this notification to specify the type, severity, and frequency of events that determine when these notifications are triggered. Some of these occurrence types require that you also enable logging in the associated policy. Note: The notification damper period specifies how often is the management server going to notify the admin with the e-mail/report data, regardless of how many events occur during that period. For example, if the damper is 1 minute and there are 3 events on 3 clients within that minute, then the management server sends one notification. Note: Add or Edit Notification Condition Note: Make sure that clients can upload critical events immediately. The Let clients upload critical events immediately option is enabled by default and configured in the Communications Settings dialog box.
Download Protection content out-of-date	Alerts the administrators about out-of-date Download Protection content. You can specify the age at which the definitions trigger the notification.
File reputation lookup alert	Alerts the administrators when a file is submitted to Symantec for a reputation check. behavioral analysis (SONAR) and Download Insight use file reputation lookups and submit files to Symantec automatically. The File Reputation Detection notification is enabled by default.
Forced application detected	This notification triggers when an application on the commercial application list is detected or when an application on the list of applications that the administrator monitors is detected.
IPS signature out-of-date	Alerts the administrators about out-of-date IPS signatures. You can specify the age at which the definitions trigger the notification.
Licensing issue	Paid license expiration This notification alerts administrators and, optionally, partners, about the paid licenses that have expired or that are about to expire. This notification is enabled by default. Over-deployment This notification alerts administrators and, optionally, partners, about over-deployed paid licenses. This notification is enabled by default. Trial license expiration This notification alerts administrators about expired trial licenses and the trial licenses that are due to expire in 60, 30, and 7 days. This notification is enabled by default if there is a trial license. It is not enabled by default if your license is due for an upgrade or has been paid.
Memory Exploit Mitigation Detection	This notification triggers when an exploit attempt against a known or unknown vulnerability is detected.
Network load alert: requests for virus and spyware full definitions	Alerts the administrators when too many clients request a full definition set, and to potential network bandwidth issues. This notification is enabled by default.
New learned application	This notification triggers when application learning detects a new application.
New risk detected	This notification triggers whenever virus and spyware scans detect a new risk.

Notification	Description
New software package	This notification triggers when a new software package downloads or the following occurs: • LiveUpdate downloads a client package. • The management server is upgraded. • The console manually imports client packages. • LiveUpdate has new security definitions or engine content. You can specify whether the notification is triggered only by new security definitions, only by new client packages, or by both. This notification is enabled by default.
New user-allowed download	This notification triggers when a client computer allows an application that Download Insight detected. An administrator can use this information to help evaluate whether to block or allow the application.
Power Eraser recommended	Alerts the administrators when a regular scan cannot repair an infection, so the administrators can use Power Eraser. This notification is enabled by default.
Risk outbreak	This notification alerts administrators about security risk outbreaks. You set the number and type of occurrences of new risks and the time period within which they must occur to trigger the notification. Types of occurrences include occurrences on any computer, occurrences on a single computer, or occurrences on distinct computers. This notification condition is enabled by default.
Server health	Server health issues trigger the notification. The notification lists the server name, the health status, the reason, and the last online or offline status. This notification is enabled by default.
Single risk event	This notification triggers upon the detection of a single risk event and provides details about the risk. The details include the user and the computer involved, and the actions that the management server took. Note: If you see one event only during the Damper time period, check the Monitors > Risk log or SONAR log for detections on multiple client computers. The damper period is designed to immediately alert the administrator only once for multiple detections.
SONAR definitions out-of-date	Alerts the administrators about out-of-date SONAR definitions. You can specify the age at which the definitions trigger the notification.
System event	This notification triggers upon certain system events and provides the number of such events that were detected. System events include management server activities, replication failures, backups, and system errors.
Unmanaged computers	This notification triggers when the management server detects unmanaged computers on the network. The notification provides details including the IP address, the MAC address, and the operating system of each unmanaged computer.
Upgrade license expiration	Upgrades from previous versions of Symantec Endpoint Protection Manager to the current version are granted an upgrade license. This notification triggers when the upgrade license is due to expire. This notification appears only after an upgrade.
Virus definitions out-of-date	Alerts the administrators about out-of-date virus definitions. You can specify the age at which the definitions trigger the notification. This notification is enabled by default.

About partner notifications

When the management server detects that clients have paid licenses that are about to expire or that have expired, it can send a notification to the system administrator. Similarly, the management server can send a notification to the administrator when it detects that licenses are over-deployed.

However, in both of these cases, the resolution of the problem may require the purchase of new licenses or renewals. In many installations the server administrator may not have the authority to make such purchases, but instead relies upon a Symantec partner to perform this task.

The management server provides the ability to maintain the contact information for the partner. This information can be supplied when the server is installed. The system administrator can also supply or edit the partner information at any time after the installation in the Licenses pane of the console.

When the partner contact information is available to the management server, paid license-related notifications and over-deployed license notifications are sent automatically both to the administrator and to the partner.

[What are the types of notifications and when are they sent?](#)

Establishing communication between the management server and email servers

For the management server to send automatic email notifications, you must configure the connection between the management server and the email server. See:

[Managing notifications](#)

To establish communication between the management server and email servers

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, select the management server for which you want to establish a connection to the email server.
3. Under **Tasks**, click **Edit the server properties**.
4. In the **Server Properties** dialog box, click the **Email Server** tab.
5. Enter the email server settings.
6. Click **OK**.

More information

[Sending test email messages fails in Endpoint Protection Manager console](#)

Viewing and acknowledging notifications

You can view unacknowledged notifications or all notifications. You can acknowledge an unacknowledged notification. You can view all the notification conditions that are currently configured in the console.

The **Security Status** pane on the **Home** page indicates the number of unacknowledged notifications that have occurred during the last 24 hours.

See [Managing notifications](#) for more information.

To view recent unacknowledged notifications	1. Click Home. 2. On the Home page, in the Security Status pane, click View Notifications. A list of recent unacknowledged notifications appears under the Notifications tab. 3. Optionally, in the list of notifications, in the Report column, click the document icon if it exists. The notification report appears in a separate browser window. If there is no document icon, all of the notification information appears in the Message column in the list of notifications.
To view all notifications	1. In the console, click Monitors and then click the Notifications tab. 2. Optionally, on the Notifications tab, from the Use a saved filter menu, select a saved filter. Saving and deleting administrative notification filters 3. Optionally, on the Notifications tab, from the Time range menu, select a time range. 4. On the Notifications tab, click View Notifications.
To acknowledge a notification	1. View notifications. 2. On the Notifications tab, in the list of notifications, in the Ack column, click the red icon to acknowledge the notification.
To view all configured notification conditions	1. In the console, click Monitors. 2. On the Monitors page, on the Notifications tab, click Notification Conditions. All the notification conditions that are configured in the console are shown. You can filter the list by selecting a notification type from the Show notification type menu.

Saving and deleting administrative notification filters

You can use filters to expand or limit your view of administrative notifications in the console. You can save new filters and you can delete previously saved filters.

For more information, see:

- [Viewing and acknowledging notifications](#)
- [Managing notifications](#)

You can create a saved filter that uses any combination of the criteria. For example, you can create a filter that only displays unacknowledged risk outbreak notifications posted during the past 24 hours.

To add a notification filter

1. In the console, click **Monitors**.
2. On the **Monitors** page, on the **Notifications** tab, click **Additional Settings**.
3. Under the **What filter settings would you like to use?** heading, set the criteria for the filter.
4. Click **Save Filter**.
5. On the **Notifications** tab, in the **Filter name** box, type a filter name, and then click **OK**.

To delete a saved notification filter

1. In the console, click **Monitors**.
2. On the **Monitors** page, on the **Notifications** tab, on the **Use a saved filter** menu, choose a filter.
3. At the right of the **Use a saved filter** menu, click the **X** icon.
4. In the **Delete Filter** dialog box, click **Yes**.

Setting up administrator notifications

You can configure notifications to alert you and other administrators when particular kinds of events occur. You can also add the conditions that trigger notifications to remind you to perform important tasks. For example, you can add a notification condition to inform you when a license has expired, or when a security risk has been detected.

When a notification triggers, it can perform specific actions, such as the following:

- Log the notification to the database.
- Send an email to one or more individuals.
- Run a batch file.

NOTE

To send email notifications, you must configure a mail server to communicate with the management server.

For more information, see:

[Establishing communication between the management server and email servers](#)

You choose the notification condition from a list of available notification types.

Once you choose the notification type, you then configure it as follows:

Specify filters	Not all notification types provide filters. When they do, you can use the filters to limit the conditions that trigger the notification. For example, you can restrict a notification to trigger only when computers in a specific group are affected.
Specify settings	All notification types provide settings, but the specific settings vary from type to type. For example, a risk notification may let you specify what type of scan triggers the notification.
Specify actions	All notification types provide actions you can specify.

NOTE

If you set the **Damper** period to **1 minute** for notifications about critical events, you should make sure that clients can upload critical events immediately. The relevant notifications include the following: **Client security alert**, **Single risk event**, **New risk detected**, and **Risk outbreak**. The **Let clients upload critical events immediately** option is enabled by default and configured in the **Communications Settings** dialog box.

To set up an administrator notification

1. In the console, click **Monitors**.
2. On the **Monitors** page, on the **Notifications** tab, click **Notification Conditions**.
3. On the **Notifications** tab, click **Add**, and then click a notification type.
4. In the **Add Notification Condition** dialog box, provide the following information:
 - In the **Notification name** text box, type a name to label the notification condition.
 - Under **What filter settings would you like to use**, if it is present, specify the filter settings for the notification condition.
 - Under **What settings would you like for this notification**, specify the conditions that trigger the notification.
 - Under **What should happen when this notification is triggered**, specify the actions that are taken when the notification is triggered.
5. Click **OK**.

More information

-
- [Managing notifications](#)
 - [Viewing and acknowledging notifications](#)

How upgrades from another version affect notification conditions

When Symantec Endpoint Protection is installed on a new server, many of the preconfigured notification conditions are enabled by default. An upgrade to Symantec Endpoint Protection from a previous version, however, can affect which notification conditions are enabled by default. It can also affect their default settings.

The following notification conditions are enabled by default in a new installation of Symantec Endpoint Protection:

- **Client list changed**
- **New client software**
- **Over deployment issue**
- **Paid license issue**
- **Risk outbreak**
- **Server health**
- **Trialware license expiration**
- **Virus definitions out-of-date**

When an administrator upgrades the software from a previous version, all existing notification conditions from the previous version are preserved. However, existing **New software package** notification conditions become **New client software** notification conditions. The **New client software** condition has two settings that are not present in the **New software package** condition: **Client package** and **Security definitions**. When the software is upgraded, both of these settings are enabled for notification conditions of this type that are preserved across the upgrade. **New client software** notifications that are conditions created after the upgrade, however, have the **Client package** setting enabled and the **Security definitions** setting disabled by default.

NOTE

When the **Security definitions** setting in the **New client software** notification condition is enabled, it may cause a large number of notifications to be sent. This situation can occur when there are many clients or when there are frequently scheduled security definition updates. If you do not want to receive frequent notifications about security definition updates, you can edit the notification condition to disable the **Security definitions** setting.

Several notification conditions may have a new setting that did not appear in earlier versions: **Send email to system administrators**. If that setting is new for a notification condition, it is disabled by default for any existing condition of that type following the upgrade.

When a default notification condition type has not been added in a previous installation, that notification condition is added in the upgraded installation. However, the upgrade process cannot determine which default notification conditions may have been deleted deliberately by the administrator in the previous installation. With one exception, therefore, all of the following action settings are disabled in each default notification condition in an upgraded installation: **Send email to system administrators**, **Log the notification**, **Run batch file**, and **Send email to**. When all four of these actions are disabled, the notification condition is not processed, even though the condition itself is present. Administrators can edit the notification conditions to enable any or all of these settings.

Note that the **New client software** notification condition is an exception: it can produce notifications by default when it is added during the upgrade process. Unlike the other default notification conditions, both the **Log the notification** and the **Send email to system administrators** action settings are enabled for this condition.

If the previous version of the software does not support licenses, an **Upgrade license expiration** notification condition is enabled.

Some notification condition types are not available in previous versions of the software. Those notification conditions are enabled by default when the software is upgraded. See:

What are the types of notifications and when are they sent?

Managing management servers, sites, and databases

Learn about client-server communication, performing disaster recovery, and configuring replication, sites, and failover.

Use this section to:

- Configure the connection between the management server and the client.
- Configure management servers and certificates.
- Manage the database.
- Set up failover and load balancing.
- Manage sites and replication.
- Perform disaster recovery.

About the types of Symantec Endpoint Protection servers

The following definitions may be helpful to understand when managing servers:

- **Site**
A site consists of one or more management servers and one database typically located together at the same business location. The site to which you log on is the local site, and you can modify it directly. Any site other than the local site is referred to as a remote site. You connect sites by using replication. See:
[Setting up sites and replication](#)
- **Management server**
The computer on which the Symantec Endpoint Protection Manager software is installed. From the management server, policies can be created and assigned to different organizational groups. You can monitor clients, view reports, logs, and alerts, and configure servers and administrator accounts. Multiple management servers at a single site provide failover and load balancing capabilities. See:
[Setting up failover and load balancing](#)
- **Database server**
The database used by Symantec Endpoint Protection Manager. There is one database per site, either the Microsoft SQL Server Express or the Microsoft SQL Server. The database can be on the same computer as the management server or on a different computer if you use a SQL Server database. SQL Server Express replaced the embedded database in 14.3 RU1. See:
[Maintaining the database](#)
- **Replication partner**
A relationship created between two sites to enable data replication between them. See:
[Setting up sites and replication](#)

Exporting and importing server settings

The server properties file includes the server settings for Symantec Endpoint Protection Manager. You may need to export and import the server properties file in the following situations:

- You use the disaster recovery file to reinstall Symantec Endpoint Protection Manager.
The disaster recovery file does not include the server settings. When you reinstall Symantec Endpoint Protection Manager, you lose any default server settings that you had previously changed. You can use the exported server properties file to reimport the changed server settings.
See: [Disaster recovery best practices for Endpoint Protection](#)
- You install Symantec Endpoint Protection Manager in a test environment and later install the management server in a production environment. You can import the exported server properties file to the production environment.

NOTE

When you import an exported domain.dat file into the same database, the domain ID changes to prevent a conflict.

To export server settings

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, expand **Local Site (Site site_name)**, and then select the management server you want to export.
3. Click **Export Server Properties**.
4. Select a location in which to save the file and specify a file name.
5. Click **Export**.

To import server settings

1. Click **Admin**, and then click **Servers**.
2. Under **Servers**, expand **Local Site (Site site_name)**, and then select the management server for which you want to import settings.
3. Click **Import Server Properties**.
4. Select the file you want to import, and then click **Import**.
5. Click **Yes**.

Managing Symantec Endpoint Protection Manager servers and third-party servers

You can configure Symantec Endpoint Protection Manager to integrate with many of the different types of servers in your network environment.

Table 184: Server management

Task	Description
Learn about servers	Decide which types of servers you need to set up. See: About the types of Symantec Endpoint Protection servers
Set server communication permissions	You can allow or deny access to the remote console. You manage access by adding exceptions based on the IP address of a single computer or a group of computers. See: Granting or blocking access to remote Symantec Endpoint Protection Manager consoles
Modify server settings	To modify database settings, or to restore your database on a different computer, you can modify server settings. See: Reinstalling or reconfiguring Symantec Endpoint Protection Manager
Configure the mail server	To work with a specific mail server in your network, you need to configure the mail server. See: Establishing communication between the management server and email servers
Manage directory servers	You can integrate Symantec Endpoint Protection with an Active Directory server and synchronize with AD groups. See: Synchronizing Active Directory groups with the Symantec Endpoint Protection Manager (SEPM)
Configure proxy settings if you use a proxy server to connect to Symantec LiveUpdate servers	To set up the Symantec Endpoint Protection Manager to connect to the Internet through a proxy server, you must configure the proxy server connection. See: Configuring Symantec Endpoint Protection Manager to connect to a proxy server to access the Internet and download content from Symantec LiveUpdate
Import or export server properties	You can export server settings to an xml file, and you can re-import the same settings. See: Exporting and importing server settings

Task	Description
Manage server certificates	The Symantec Endpoint Protection Manager server uses a server certificate to encrypt data for the communication between all servers, and clients in a network. The server identifies and authenticates itself with a server certificate. You may need to back up, update, or generate a new server certificate. See: • About server certificates • Updating or restoring a server certificate • Backing up a server certificate • Generating a new server certificate
Configure SecurID Authentication for a server	If you choose to authenticate administrator accounts by using RSA SecurID, you must also configure the management server to communicate with the RSA server. See: Using RSA SecurID authentication with Symantec Endpoint Protection Manager
Configure two-factor authentication for Symantec Endpoint Protection Manager with Symantec VIP	If you use Symantec VIP in your environment for two-factor authentication, you can enable it for those administrators who authenticate with Symantec Endpoint Protection Manager Authentication. This support is added in version 14.2. For more information, see: Configuring two-factor authentication with Symantec VIP
Move the server to a different computer	You may need to move the management server software from one computer to another for the following reasons: • You must move the management server from a test environment to a production environment. • The computer on which the management server runs has a hardware failure. You can move the management server software in the following ways: • Install the management server on another computer and perform replication. See: How to install a second site for replication • Install the management server on another computer using the recovery file. See: Reinstalling or reconfiguring Symantec Endpoint Protection Manager
Start and stop the management server	The management server runs as an automatic service. You must stop the management server service when you upgrade, or perform disaster recovery. See: Stopping and starting the management server service

Maintaining the database

Symantec Endpoint Protection (SEPM) supports both the Microsoft SQL Server Express database and the Microsoft SQL Server database. If you have more than 5,000 clients, use a Microsoft SQL Server database.

Symantec Endpoint Protection Manager automatically installs the Microsoft SQL Server Express database. You can also install SQL Server Express separately. The database contains information about security policies, configuration settings, attack data, logs, and reports. SQL Server Express replaced the embedded database in 14.3 RU1.

After you install Symantec Endpoint Protection Manager, the management server may start to slow down after a few weeks or a few months. To improve the management server performance, you may need to reduce the database storage space and schedule various database maintenance tasks.

Table 185: Database management tasks

Task	Description
Schedule regular database backups	You should schedule regular database backups in case the database gets corrupted. See: • Backing up the database and logs • Scheduling automatic database backups • Disaster recovery best practices for Endpoint Protection Optionally, to prevent an automatic sweep of the database until after a backup occurs, you can manually sweep data from the database. See: Clearing log data from the database manually
Schedule database maintenance tasks	You can speed up the interaction time between the management server and the database by scheduling database maintenance tasks. You can schedule the management server to perform the following maintenance tasks immediately or when users are not on the client computers. • Remove unused data from the transaction log. • Rebuild the database table indexes to improve the database's sorting and searching capabilities. For more information, see: Scheduling automatic database maintenance tasks
Periodically check the database file size	Make sure that the database does not reach the maximum file size. The Microsoft SQL Server Express database has a 10 GB size limit. If you install SQL Server Express when you install SEPM, SEPM warns you if you approach the limit. See: Increasing the Microsoft SQL Server database file size
Calculate the database storage space that you need	Before you can decide how to reduce the amount of storage space, calculate the total amount of disk space that you need. The database storage is based on the following factors: • Log size and expiration time period. • The number of client computers. • The average number of viruses per month. • The number of events you need to retain for each log. • The number of content updates. The content updates require about 300 MB each. See: – Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager – Reverting to an older version of the Symantec Endpoint Protection security updates • The number of client versions you need to retain for each language. For example, if you have both 32-bit clients and 64-bit clients, you need twice the number of language versions. • The number of backups you need to keep. The backup size is approximately 75 percent of the database size, and then multiplied by the number of backup copies that you keep. For more information on how to calculate the hard disk space you need, see the following Symantec white paper: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper

Task	Description
Reduce the volume of log data	The database receives and stores a constant flow of entries into its log files. You must manage the data that is stored in the database so that the stored data does not consume all the available disk space. Too much data can cause the computer on which the database runs to crash. You can reduce the volume of log data by performing the following tasks: • Upload only some of the client logs to the server, and change the frequency with which the client logs are uploaded. See: Specifying client log size and which logs to upload to the management server • Specify how many log entries the client computer can keep in the database, and how long to keep them. See: Specifying the log size and how long to keep log entries in the database • Filter the less important risk events and system events out so that less data is forwarded to the server. See: Modifying log handling and notification settings on Windows computers • Reduce the amount of space in the directory where the log data is stored before being inserted into the database. See: About increasing the disk space on the server for client log data • Reduce the number of clients that each management server manages. See: Configuring a management server list for load balancing • Reduce the heartbeat frequency, which controls how often the client logs are uploaded to the server. See: Updating policies and content on the client using push mode or pull mode
Export log data to another server	For security purposes, you might need to retain the number of log records for a longer period of time. To keep the client log data volume low, you can export the log data to another server. You can configure multiple management servers to receive log data in case one server goes down. See: • Exporting data to a Syslog server • Exporting log data to a text file
Create client installation packages with only the protection that you need	The more protection features that you install with the client, the more space that the client information takes in the database. Create the client installation package with only the appropriate level of protection the client computer needs. The more groups you add, the more space the client information takes in the database. See: Choosing which security features to install on the client
Use the Group Update Provider to download content	If you have low bandwidth or more than 100 client computers, use Group Update Providers to download content. For example, 2,000 clients using a Group Update Provider is the equivalent of using four to five management servers to download content. See: Using Group Update Providers to distribute content to clients To reduce disk space and database size, you can reduce the number of content revisions that are kept on the server. See: Downloading content from LiveUpdate to the Symantec Endpoint Protection Manager
Restore the database	You can recover a corrupted database by restoring the database on the same computer on which it was installed originally. Or, you can install the database on a different computer. See: Restoring the database

The information in the database is stored in tables, also called the database schema. You might need the schema to write queries for customized reports. For more information, see:

[Symantec Endpoint Protection Manager Database Schema Reference](#)

More information

[Verifying the connection with the database](#)

Running automatic database backups

You can schedule database backups to occur at a time when fewer users are logged on to the network.

You can also back up the database at any time. See:

[Backing up the database and logs](#)

To run automatic database backups

1. In the console, click **Admin > Servers**.
2. Under **Servers**, click **Local Site (My Site) > SQLEXPRESSSYMC**.
3. Under **Tasks**, click **Edit Database Properties**.
4. In the **Database Properties** dialog box, on the **Backup Settings** tab, do the following tasks.
 - In the **Backup server** drop-down list, specify on which management server you want to save the backup.
 - Check **Back up logs** if you need to save a copy of the logs for security purposes or company policy. Otherwise, leave this option disabled, as logs use a lot of disk space.
 - Set the **Number of backups to keep** if your company policy requires it. Keep the number low if you use the default database and your database size is too large.
5. Make sure **Schedule Backups** is checked, and set the schedule.
6. Click **OK**.

Scheduling automatic database maintenance tasks

After you install the management server, the space in the database grows continually. The management server slows down after a few weeks or months. To reduce the database size and to improve the response time with the database, the management server performs the following database maintenance tasks:

- Truncates the transaction log.
The transaction log records almost every change that takes place within the database. The management server removes unused data from the transaction log.
- Rebuilds the index.
The management server defragments the database table indexes to improve the time it takes to sort and search the database.

By default, the management server performs these tasks on a schedule. You can perform the maintenance tasks immediately, or adjust the schedule so that it occurs when users are not on their computers.

NOTE

You can also perform the database maintenance tasks in Microsoft SQL Server Management Studio. However, you should perform these tasks in either Symantec Endpoint Protection Manager or Management Studio, but not both.

To run database maintenance tasks on demand

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, click the icon that represents the database.
3. Under **Tasks**, select either of the following options:
 - **Truncate Transaction Log Now**
 - **Rebuild Indexes Now**
4. Click **Run**.
5. After the task completes, click **Close**.

To schedule database maintenance tasks to run automatically

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, click the icon that represents the database.
3. Under **Tasks**, click **Edit Database Properties**.
4. On the **General** tab, check either or both of the following options, then click **Schedule Task** and specify the schedule for each task.
 - **Truncate the database transaction logs**. The default schedule for this task is every four hours.
 - **Rebuild Indexes**. The default schedule for this task is every Sunday at 2:00.

WARNING

If you perform these tasks in SQL Server Management Studio, uncheck these options.

More information

[Scheduling automatic database backups](#)

Increasing the Microsoft SQL Server database file size

If you use the SQL Server database, periodically check the database size to make sure that the database does not reach its maximum size. If you can, increase the maximum size that the SQL Server database holds. See:

[Scheduling automatic database maintenance tasks](#)

To increase the Microsoft SQL Server database size

1. On the Microsoft SQL server computer, open the SQL Server Management Studio.
2. In the Object Explorer, Expand the "Databases" folder, right-click **sem5**, and click **Properties**.
3. In the **Database Properties** dialog box, select **Files**.
4. Under **Database files**, select **sem5_log1**, and scroll to the right to view the **Autogrowth** column.
5. In the **Autogrowth** column, click the ... button.
6. In the **Change Autogrowth for sem5_log1** dialog box, click **Unrestricted File Growth**, and then click **OK**.
7. Click **OK**.

Specifying client log size and which logs to upload to the management server

Company policy might require you to increase the time and type of log events that the database keeps. You can specify the number of log entries that are kept, and the number of days that each entry is kept on the client.

You can configure whether to upload each type of client log to the server. You can also configure the maximum upload size. If you choose not to upload the client logs, you cannot perform the following tasks:

- You cannot view the client log data from the Symantec Endpoint Protection Manager console by using the **Logs** tab on the **Monitors** page.
- You cannot back up the client logs when you back up the database.
- You cannot export the client log data to a file or a centralized log server.

NOTE

Some client log settings are group-specific and some are set in the Virus and Spyware Protection policy, which can be applied to a location. If you want all remote client log and office client log settings to differ, you must use groups instead of locations to manage remote clients.

For more information, see:

[Specifying the log size and how long to keep log entries in the database](#)

To specify client log size and which logs to upload to the management server

1. On the console, click **Clients**, and select a group.
2. On the **Policies** tab, click **Client Log**.
3. In the **Client Log Settings** for group name dialog box, set the maximum file size and the number of days to keep log entries.
4. Check **Upload to management server** for any logs that you want the clients to forward to the server.
5. For the **Security** log and **Traffic** log, set the damper period and the damper idle period.
6. Click **OK**.

Specifying the log size and how long to keep log entries in the database

To help control hard disk space, you can decrease the number of log entries that the database keeps. You can also configure the number of days the entries are kept.

NOTE

Log information on the Symantec Endpoint Protection Manager console **Logs** tab on the **Monitors** page is presented in logical groups for you to view. The log names on the **Site Properties Log Settings** tab correspond to log content rather than to log types on the **Monitors** page **Logs** tab.

For more information, see:

[Specifying client log size and which logs to upload to the management server](#)

To specify the log size and how long to keep log entries in the database

1. In the console, click **Admin**.
2. Under **Servers**, expand **Local Site**, and click the database.
3. Under **Tasks**, click **Edit Database Properties**.
4. On the **Log Settings** tab, set the number of entries and number of days to keep log entries for each type of log.
5. Click **OK**.

About increasing the disk space on the server for client log data

A configuration that uploads a large volume of client log data to the server at frequent intervals can cause disk space problems on the server. If you must upload a large volume of client log data, you may have to adjust some default values to avoid these space problems. As you deploy to clients, you should monitor the space on the server in the log insertion directory and adjust these values as needed.

The default directory where the logs are converted to .dat files and then written to the database is in the following default location:

`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\inbox\log.`

To adjust the values that control the space available on the server, you must change these values in the Windows registry. The Windows registry keys that you need to change are located on the server in: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Symantec\Symantec Endpoint Protection\SEPM`

The following table lists the Windows registry keys and their default values and describes what they do.

Table 186: Windows registry keys that contain log upload settings

Value name	Description
MaxInboxSpace	Specifies the space that is allotted for the directory where log files are converted to .dat files before they are stored in the database. The default value is 8 GB.
MinDataFreeSpace	Specifies the minimum amount of space that should be kept free in this directory. This key is useful to ensure that other applications that use the same directory have enough space to run without an adverse effect on performance. The default value is 200 MB.
IntervalOfInboxSpaceChecking	Specifies how long the management server waits before it checks on the amount of space in the inbox that is available for log data. The default value is 30 seconds.

More information

[Maintaining the database](#)

Clearing log data from the database manually

You can perform a manual log sweep after backing up the database, if you prefer to use this method as part of routine database maintenance.

If you allow an automatic sweep to occur, you may lose some log data if your database backups do not occur frequently enough. If you regularly perform a manual log sweep after you have performed a database backup, it ensures that you retain all your log data. This procedure is very useful if you must retain your logs for a relatively long period of time, such as a year. You can manually clear the logs, but this procedure is optional and you do not have to do it. See:

- [Backing up the database and logs](#)
- [Specifying the log size and how long to keep log entries in the database](#)

To clear log data from the database manually

1. To prevent an automatic sweep of the database until after a backup occurs, increase a site's log size to their maximums.
2. Perform the backup, as appropriate.
3. On the computer where the manager is installed, open a Web browser and type the following URL:

`https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs`

After you have performed this task, the log entries for all types of logs are saved in the alternate database table. The original table is kept until the next sweep is initiated.

4. To empty all but the most current entries, perform a second sweep. The original table is cleared and entries then start to be stored there again.
5. Return the settings on the **Log Settings** tab of the **Site Properties** dialog box to your preferred settings.

Setting up failover and load balancing

The client computers must be able to connect to a management server at all times to download the security policy and to receive log events. You should set up failover to maintain communication with a Symantec Endpoint Protection Manager when the management server becomes unavailable. Load balancing is used to distribute client management between multiple management servers using a management server list.

The following table lists the tasks that you should perform to set up failover and load balancing.

Table 187: Process for setting up failover and load balancing

Tasks	Description
Read about failover and load balancing.	You should understand if and when you need to set up management servers for failover and load balancing. See: About failover and load balancing
Install additional management servers.	For more information, see: Installing a management server for failover or load balancing The number of clients for each management server depends on several factors, such as the log sizes. To calculate how many management servers you need, see: Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper
Add management servers to a management server list.	To set up load balancing, you add multiple management servers to a management server list. You can either use the default management server list or add management servers to a new management server list. A management server list includes the IP addresses or host names of management servers to which clients can connect. See: Configuring a management server list for load balancing
Assign the custom management server list to a group.	After you have created a custom management server list, you must assign the management server list to a group. See: Assigning a management server list to a group and location

If the management server goes offline, or the client and the management server do not communicate, you should also troubleshoot the problem. See:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

More information

[Configuring a failover server for external logging](#)

[Setting up sites and replication](#)

About failover and load balancing

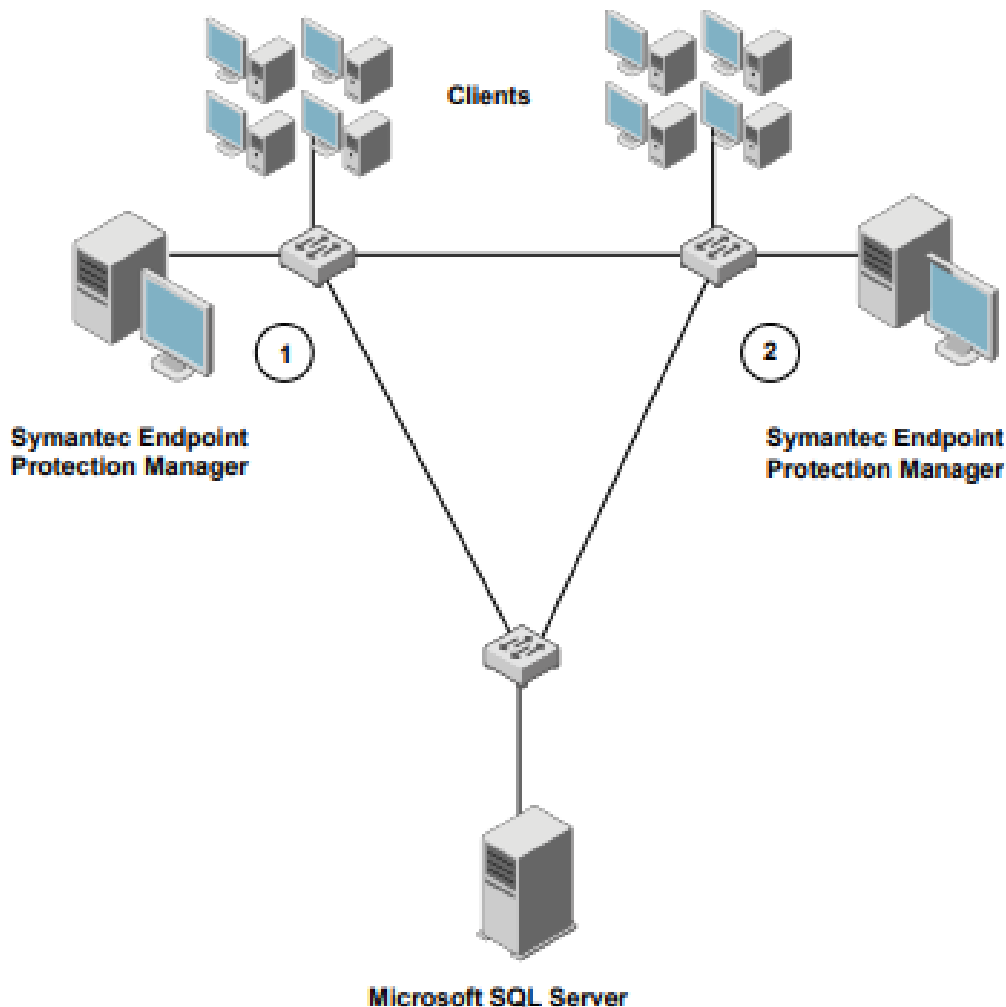
You can install two or more management servers that communicate with one database and configure them for failover or load balancing. Failover redirects the workload to a backup management server when the main server fails. Load balancing distributes workloads to prevent one management server from being overloaded.

How does failover and load balancing work?

Failover occurs when you install more management servers than are required to handle your clients to protect against the failure of an individual management server. *Load balancing* occurs with a prioritized list of management servers that is assigned to a group. You should add at least two management servers to a site to automatically distribute the load among them.

In a custom management server list, each server is assigned to a priority level. A client that comes onto the network selects a priority one server to connect to at random. If the first server it tries is unavailable and there are other priority one servers in the list, it randomly tries to connect to another. If no priority one servers are available, then the client tries to connect to one of the priority two servers in the list. This method of distributing client connections randomly distributes the client load among your management servers.

The following diagram shows components on different subnets. Management servers and database servers can be on the same subnets. The servers are identified with the numbers 1 and 2, which signify a failover configuration.



In a failover configuration, all clients send traffic to and receive traffic from server 1. If server 1 goes offline, all clients send traffic to and receive traffic from server 2 until server 1 comes back online. The database is illustrated as a remote installation, but it also can be installed on a computer that runs the Symantec Endpoint Protection Manager.

Which Symantec Endpoint Protection components use failover?

For multiple Symantec Endpoint Protection Managers in a site, you can use failover in the following situations.

- **Content updates** All the components that run LiveUpdate can also use a prioritized list of update sources. Your management servers can use a local LiveUpdate server and failover to LiveUpdate servers in other physical locations.

NOTE

The use of internal LiveUpdate servers, Group Update Providers, and site replication does not provide the load balancing functionality. You should not set up multiple sites for load balancing.

- **Databases:** If you use a Microsoft SQL Server database or Microsoft SQL Server Express database, you can set up failover and load balancing. For 14.3 MPx and earlier you can set up failover with the Microsoft SQL Server database. You can set up failover with the embedded database but only if you use replication. When you use replication with an

embedded database, Symantec recommends that you do not configure load balancing, as data inconsistency and loss may result.

- **Reporting:** Reporting tasks run on one management server. If the server goes down, the `semapisrv` service checks that the second management server has internet connectivity. If the second management server has connectivity, failover occurs.
- **Hybrid management:** In 14.3 RU7 and earlier, you cannot set up failover with the cloud server. In 14.3 RU8, if the higher priority management server goes down, the `semapisrv` service checks whether a second management server has internet connectivity. If the second management server has connectivity, it runs the cloud connector and tries to connect to the cloud server. If the connectivity check fails, failover fails and the process starts over with a third management server. Regardless of which management server connects to the cloud, the same domain stays enrolled with the cloud server.

More information

- [Setting up failover and load balancing](#)
- [Configuring a management server list for load balancing](#)
- [Determining how many sites you need](#)
- [Setting up sites and replication](#)

Configuring a management server list for load balancing

By default, the management servers are assigned the same priority when configured for failover and load balancing. If you want to change the default priority after installation, you can do so by using the Symantec Endpoint Protection Manager console. You can only configure load balancing when a site includes more than one management server.

Load balancing occurs between the servers that are assigned to priority 1 in a management server list. If more than one server is assigned to priority 1, the clients randomly choose one of the servers and establish communication with it. If all priority 1 servers fail, clients connect with the server assigned to priority 2.

To provide both load balancing and roaming:

- Enable DNS and put a domain name as the only entry in a custom management server list.
- Enable the Symantec Endpoint Protection location awareness feature and use a custom management server list for each location. Create at least one location for each of your sites.
- Use a hardware device that provides failover or load balancing. Many of these devices also offer a setup for roaming.

For more information, see:

[About failover and load balancing](#)

To configure a management server list for load balancing

1. In the console, click **Policies**.
2. Expand **Policy Components**, and then click **Management Server Lists**.
3. Under **Tasks**, click **Add a Management Server List**.
4. In the **Management Server Lists** dialog box, click **Add > New Server**.
5. In the **Add Management Server** dialog box, in the **Server Address** box, type the fully qualified domain name or IP address of a management server.

If you type an IP address, be sure that it is static, and that all clients can resolve it.

-
6. Click **OK**.
 7. Add any additional servers.
 8. To configure load balancing with another management server, click **Add > New Priority**.
 9. To change the priority of a server for load balancing, select a server, and then click **Move Up** or **Move Down**.
 10. Click **OK**.

You must then apply the management server list to a group. See:

[Assigning a management server list to a group and location](#)

Installing a management server for failover or load balancing

Failover configurations are used to maintain communication when clients cannot communicate with a Symantec Endpoint Protection Manager. Load balancing is used to distribute client management between management servers. You can configure failover and load balancing by assigning priorities to management servers in management server lists.

Failover and load balancing installations are supported only when the original Symantec Endpoint Protection Manager uses a Microsoft SQL Server database. The SQL Server Native Client files also must be installed on the computer that you use for failover or load balancing.

To install a management server for failover or load balancing:

1. Install a Symantec Endpoint Protection Manager. See:
[Installing Symantec Endpoint Protection Manager](#)
2. In the **Management Server Configuration Wizard** panel, check **Custom Configuration**, and then click **Next**. See:
[Configuring Symantec Endpoint Protection Manager after installation](#)
3. Select the number of clients you expect the server to manage, and then click **Next**.
4. Check **Install an additional management server to an existing site**, and then click **Next**.
5. In the server information panel, accept or change the default values, and then click **Next**.
6. In the **Microsoft SQL Server Information** dialog box, click **OK** in the message about installing the SQL Server client tools.
7. Enter the remote server values for the following text boxes:

Step One tells the Symantec Endpoint Protection Manager where to find the SQL Server on the network, which includes host name, instance name, and port.

You also pick the authentication type, including Windows Authentication or SQL authentication.

- **Database server** \instance_name
SQL server port
Database name
SQL client folder (on the local computer)
If this text box does not automatically populate with the correct path, the Microsoft SQL Client Utility is not installed or it is not installed correctly.

8. **Step Two** tells the Symantec Endpoint Protection Manager how to authenticate to the SQL Server and includes the database name, database user, and database user's password.

You should have had this information available already for when you installed the first management server for that site.

-
9. Click **Next**.
 10. Specify and confirm a password for the Symantec Endpoint Protection Manager admin account.
Optionally, provide an administrator email address.
 11. Click **Next**.
 12. At the warning, read the text message, and then click **OK**.
 13. In **Management Server Completed** panel, click **Finish**. See:

[Configuring a failover server for external logging](#)

Assigning a management server list to a group and location

After you add a policy, you must assign it to a group or a location or both. You can also use the management server list to move a group of clients from one management server to another.

You must have finished adding or editing a management server list before you can assign the list. See:

[Configuring a management server list for load balancing](#)

To assign a management server list to a group and location

1. In the console, click **Policies**.
2. In the **Policies** page, expand **Policy Components**, and then click **Management Server Lists**.
3. In the **Management Server Lists** pane, select the management server list you want to assign.
4. Under **Tasks**, click **Assign the List**.
5. In the **Apply Management Server List** dialog box, check the groups and locations to which you want to apply the management server list.
6. Click **Assign**.
7. Click **Yes**.

To assign a management server list to a group or location on the Clients page

1. In the console, click **Clients > Policies**.
2. On the **Policies** tab, select the group, and then uncheck **Inherit policies and settings from parent group**.
You cannot set any communication settings for a group unless the group no longer inherits any policies and settings from a parent group.
3. Under **Location-independent Policies and Settings**, click **Communication Settings**.
4. In the **Communication Settings for group name** dialog box, under **Management Server List**, select the management server list.
The group that you select then uses this management server list when communicating with the management server.
5. Click **OK**.

Replacing a management server list

For load balancing, you create a second management server list, and then either assign it to the original groups or replace it. For example, suppose you have three lists, **Default Management Server List**, List2, and List3. You can replace **Default Management Server List** with List3, but you cannot replace List2 with List3 at the same time. Instead, you can replace both **Default Management Server List** and List2 at the same time by using the **Assign the List** command.

See: [Assigning a management server list to a group and location](#)

To replace a management server list with a different list

1. Created a second management server list.
See: [Configuring a management server list for load balancing](#)

2. On the **Policies** page, click **Policy Components > Management Server Lists**.
3. Under **Tasks**, click **Replace the List...**
4. In the **Replace Management Server List** dialog box, choose the new list from the **New Management Server list** drop-down list, and select the groups you want to apply the new list to.
The groups in bold display the current management server list.
You cannot replace a list for a group that inherits from a parent group. Groups that inherit display the following text: **[inherit from the parent group]**.
5. Click **Replace > Yes**.

Setting up sites and replication

A site consists of one database, one or more management servers, and clients. By default, you deploy Symantec Endpoint Protection as a single site. Organizations with more than one data center or physical location generally use multiple sites.

Replication configurations are used for redundancy. Data from one database is duplicated, or replicated, on another database. If one database fails, you can still manage and control all clients because the other database contains the client information. See:

[What are sites and how does replication work?](#)

Table 188: Process for setting up sites and replication

Tasks	Description
Step 1: Determine whether you need to add another site	Before you set up multiple sites and replication, make sure that it is necessary. Symantec recommends that you set up multiple sites only in specific circumstances and that you add a maximum of five sites in each site farm. If you do add an additional site, decide which site design works for your organization. See: Deciding whether or not to set up multiple sites and replication Determining how many sites you need
Step 2: Install Symantec Endpoint Protection Manager on the first site	When you install Symantec Endpoint Protection for the first time, by default you have installed the first site, or the local site. See: Installing Symantec Endpoint Protection Manager
Step 3: Install Symantec Endpoint Protection Manager on the second site	You create a second site by installing a second management server. The second site is classified as a remote site and the management server is called a replication partner. Replication occurs according to the default schedule that when you added the second site during the initial installation. After you have added a replication partner, you can change the replication schedule and what data is replicated. See: How to install a second site for replication The first time that the databases between the two sites replicate, let the replication finish completely. The replication may take a long time because the entire database gets replicated. You may want to replicate the data immediately, rather than waiting until the database are scheduled to replicate. You can also change the replication schedule to occur earlier or later. If you upgrade the management server on one site, you must upgrade the management server version on all sites. See: Replicating data immediately

Tasks	Description
Step 4: Check the history for replication events (optional)	If you need to check that the replication occurred or to troubleshoot the replication events, look at the System log. In the second management server, view the System log. Filter for the Administrative > Replication events event type. For more information, see: Viewing logs

You can also reconfigure a management server to replicate the data with a currently existing site in your network. Or, if you have two non-replicating sites, you can convert one of the sites into a site that replicates with the second site. See:

[Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)

Note the following:

- After you configure the Symantec Endpoint Protection, you should back up the database, which contains all your configuration changes. See:
[Backing up the database and logs](#)
- If you disable a replication partner to upgrade to the latest version of the management server, you must re-add the replication partner. See:
 - [Disabling replication and restoring replication before and after an upgrade](#)
 - [Upgrading to a new release](#)

More information

[Connecting to a directory server on a replicated site](#)

What are sites and how does replication work?

Refer to the following topics for more information:

Sites and replication partners

A site is a Symantec Endpoint Protection Manager database with one or more Symantec Endpoint Protection Managers attached to that database. Replication enables data to be duplicated between databases on separate sites so that both databases contain the same information. If one database fails, you can manage each site by using the information on the database from the second site.

A replication partner is an individual management server within the second site, or remote site. A site may have as many replication partners as needed. Each partner connects to the main site or local site, which is the site that you are logged on to. All sites that are set up as partners are considered to be in the same site farm.

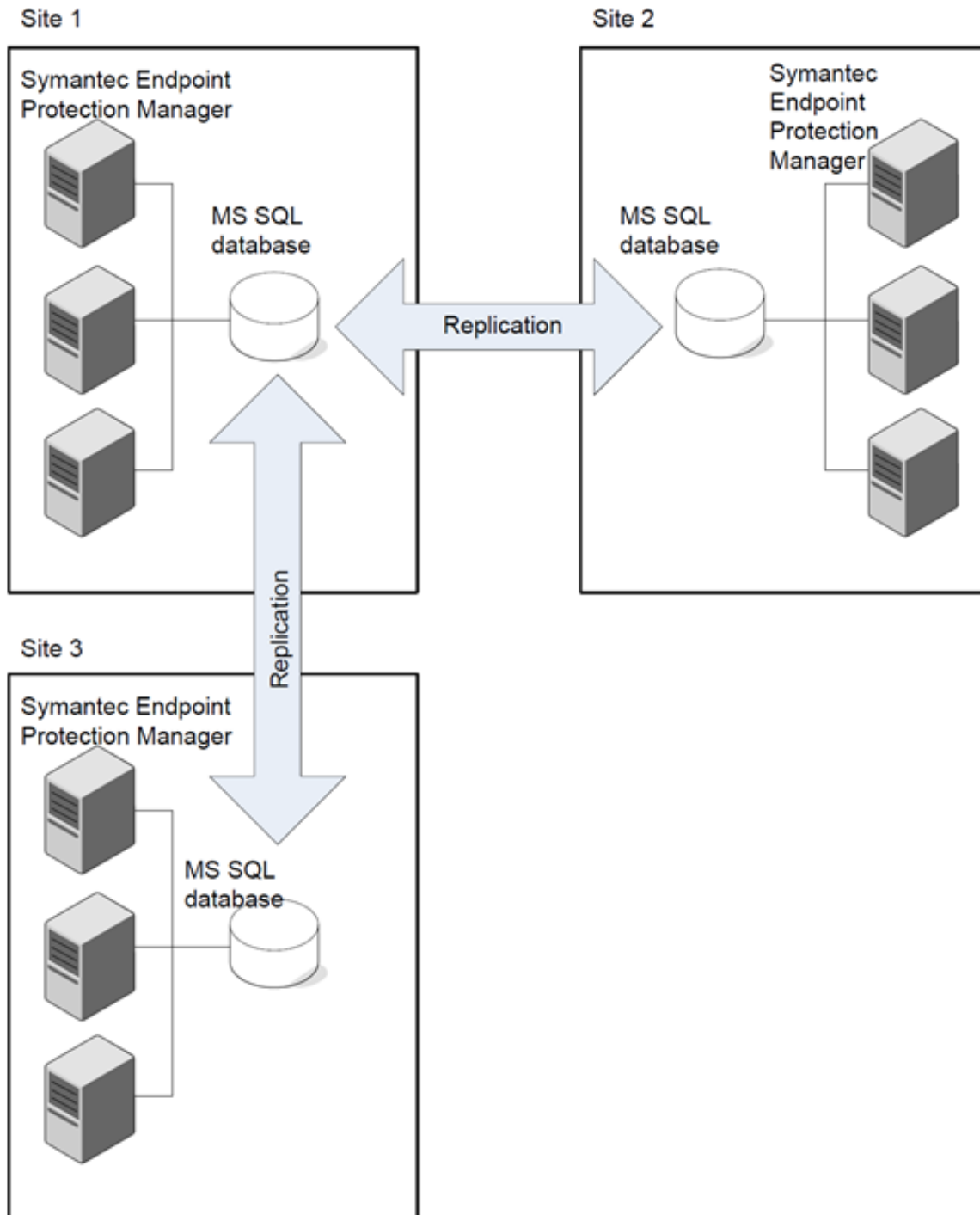
Each site you replicate data with is either a replication partner or a site partner. Both replication partners and site partners use multiple management servers, but the database they use and the way in which they communicate is different:

- Replication partners can use either the default database (Microsoft SQL Server Express in 14.3 RU1) or a Microsoft SQL Server database. The management servers do not share the database. All replication partners share a common license key. If you use the Microsoft SQL Server database, you can connect multiple management servers that share one database. Only one of the management servers needs to be set up as a replication partner.
- Site partners share a single Microsoft SQL Server database.

How does replication work?

The changes that you make on any partner are duplicated to all other partners. For example, you may want to set up one site at your main office (site 1) and a second site (site 2). Site 2 is a partner to site 1. The databases on site 1 and site 2 are reconciled by using the replication schedule. If a change is made on site 1, it automatically appears on site 2 after replication occurs. If a change is made on site 2, it automatically appears on site 1 after replication occurs. You can also install a third site (site 3) that can replicate data from either site 1 or site 2.

After replication occurs, the database on site 1 and the database on site 2 are the same. Only computer identification information for the servers differs.



For more information on how often to replicate, see the following article:

[SEPM Replication Setup](#)

For more information, see:

-
- [Deciding whether or not to set up multiple sites and replication](#)
 - [Determining how many sites you need](#)
 - [How to resolve data conflicts between sites during replication](#)

Determining the size of the replication server

A replication partner requires a larger database than a single management server installation. The increased size requirements for the replication server include the following factors:

- Number of managed clients
- Client installation package sizes retained in the database
- Number of log files retained
- Database maintenance settings
- Log size and expiration timeframes
- Definition update sizes
- Database backup information requirements

In general, the hard disk requirements for the replication server should be at least three times the hard disk space used by the original Symantec Endpoint Protection Manager for the initial replication.

More information

- [How to install a second site for replication](#)
- [Replication considerations and best practices](#)
- [Symantec Endpoint Protection Sizing and Scalability Best Practices White Paper](#)

How to resolve data conflicts between sites during replication

Replication causes data to be transferred or forwarded to another management server. Sites can have multiple replication partners, and any changes made on one partner are replicated to all sites.

What data is duplicated?

Neither replication site overrides the other. Instead they compare what each site has, and if one site has a package or piece of content the other does not, then it is shared. If all LiveUpdate content and client packages match up, then nothing is exchanged.

The replication partners duplicate the following data:

- Policies and groups (required bidirectional)
- LiveUpdate content and client installation packages, if you specify these options (optional bidirectional)
- Logs (optional bidirectional or unidirectional)

If you upgrade the management server on one site, you must upgrade the management server version on all sites. Replication does not occur if the database schema versions do not match.

The following table describes how the management server resolves conflicts if administrators change settings on the sites in a site farm.

Table 189: How the management server resolves conflicts between sites

Conflict type	Example	Resolution
Two differences cannot exist together.	Administrators for site 1 and site 2 both configure an identical Firewall policy setting. On site 1, the setting is enabled. On site 2, the setting is disabled.	The management server retains only the most recently made change. For example, if you made a change on site 1 first, and site 2 second, then the site 2 change is retained.
The same variable is created for both sites.	Administrators on site 1 and site 2 both add a group with the same name.	The management server retains both changes, adding a tilde and the numeral 1 (~1) after the more recently made variable. For example, with two groups named as Sales, the most recently named Sales group becomes Sales ~1.
Data can merge without conflict.	The administrator for site 1 adds two Firewall policies and the administrator for site 2 adds five Firewall policies.	The management server merges the changes. For example, the management server displays all seven Firewall policies on both sites.

Deciding whether or not to set up multiple sites and replication

Before you install a second site, you should decide whether or not multiple sites and replication are a good choice in your network. Setting up more than one site adds a complexity that you may not need. Multiple sites can cause certain tasks such as viewing client logs and reports more difficult. Generally, you should install only one site.

The main purposes to set up multiple sites and replication are:

- If your network has a slow WAN link.
Multiple sites provide a second management server to which clients in multiple geographical areas can connect locally. For example, suppose a company has several large offices in both Germany and in the United States. If the connection between Germany and the United States is slow, then the company should create one site in Germany and one site in the United States. The Germany clients can connect to the Germany site and the United States clients can connect to the United States site. This distribution reduces the number of clients that have to communicate over the slow WAN link.
- For database redundancy.
Replication ensures that if one datacenter was corrupted or lost, you would have backed up the database in a different datacenter.

In some situations, you should use a Group Update Provider (GUP) instead of multiple sites and replication. Use a GUP when you have either a lot of clients, or clients that are distributed over several geographical locations.

NOTE

You should not set up more than five replicated sites.

Table 190: Deciding whether to use more than one site with replication, a GUP, or neither

Question	Answer	Use multiple sites with replication or use a GUP
Do you have more than 45,000 clients?	Yes. Do you have either multiple locations or a slow WAN link that connects to a location with more than 1,000 clients?	Yes. • For a slow WAN link, consider using replication. • For multiple locations, consider using a GUP.
		No. You do not need either replication or a GUP.

Question	Answer	Use multiple sites with replication or use a GUP
	No.	Yes. Consider using replication.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.
Do you have a slow WAN link?	Yes.	Yes. Consider using replication.
	Do you have multiple locations with more than 1,000 clients per location?	No. Consider using a GUP.
	No.	Yes. Consider using replication.
	Do you have multiple locations with more than 1,000 clients per location?	No. You do not need either replication or a GUP.
Do you have multiple locations with more than 1,000 clients per location?	Yes.	Yes. Consider using a GUP.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.
	No	Yes. Consider using a GUP.
	Do you have a slow WAN link that connects to a location with more than 1,000 clients?	No. You do not need either replication or a GUP.

More information

- [When to use replication with Symantec Endpoint Protection Manager](#)
- [Using Group Update Providers to distribute content to clients](#)
- [Setting up sites and replication](#)
- [Determining how many sites you need](#)

Determining how many sites you need

A majority of small and medium-sized organizations need only a single site to centrally manage network security. Since each site has only one database, all data is centrally located.

Even a large organization with a single geographic location typically needs only needs one site. But for the organizations that are too complex to manage centrally, you should use a distributed management architecture with multiple sites.

You should consider multiple sites for any of the following factors:

- A large number of clients.
- The number of geographical locations and the type of communications links between them.
- The number of functional divisions or administrative groups.
- The number of datacenters. A best practice is to set up one Symantec Endpoint Protection site for each datacenter.
- How frequently you want to update the content.
- How much client log data you need to retain, how long you need to retain it, and where it should be stored.
- A slow WAN link between multiple physical locations with thousands of clients. If you set up a second site with its own management server, you can minimize the client-server traffic over that slow link. With fewer clients, you should use a Group Update Provider. See: [Using Group Update Providers to distribute content to clients](#)
- Any miscellaneous corporate management and IT security management considerations that are unique.

Use the following size guidelines to decide how many sites to install:

- Install as few sites as possible, up to a maximum of 20 sites. You should keep the number of replicated sites under five.
- Connect up to ten management servers to a database.
- Connect up to 18,000 clients to a management server.

After you add a site, you should duplicate site information across multiple sites by replication. Replication is the process of sharing information between databases to ensure that the content is consistent.

Table 191: Multi-site designs

Site design	Description
Distributed	Each site performs replication bi-directionally for groups and policies, but not logs and content. To view the site reports, you use the console to connect to a management server in the remote site. Use this design when you do not need immediate access to remote site data.
Centralized logging	All logs are forwarded from the other sites to a central site. Use this design when you require centralized reporting.
High availability	Each site has multiple management server installations and database clustering. To handle additional clients, you add multiple management servers rather than adding multiple sites. You then use a management server list to configure client computers to automatically switch to an alternative management server if the primary management server becomes unavailable. You use this design to provide redundancy, failover, and disaster recovery. Note: When you use replication with an embedded database (14.3 MPx and earlier), Symantec recommends that you do not add load balancing, as data inconsistency and loss may result. For more information, see: Setting up failover and load balancing

For more information on whether or not to set up replication, see the following article:

[When to use replication with Endpoint Protection Managers](#)

More information

- [What are sites and how does replication work?](#)
- [Setting up sites and replication](#)
- [Deciding whether or not to set up multiple sites and replication](#)

How to install a second site for replication

Installing a second site for replication is a two-part process:

- Install a second Symantec Endpoint Protection Manager and database to replicate with a Symantec Endpoint Protection Manager and database that is already installed.
- Log on to the second Symantec Endpoint Protection Manager and change the schedule and the items that you want to replicate (optional). See:

[Changing the replication frequency and content](#)

To install a second site for replication

1. Install a second Symantec Endpoint Protection Manager. See:
[Installing Symantec Endpoint Protection Manager](#)
The **Management Server Configuration Wizard** automatically starts after the management server installation.
2. In the **Management Server Configuration Wizard**, click **Custom configuration for new installation (more than 500 clients, or custom settings)**, and then click **Next**.
3. Click **Install an additional site**, and then click **Next**.
4. In the next panel, type the following information, and then click **Next**:
 - **Replication server**

The name or IP address of the management server that is already installed and that this management server replicates with.

– **System Administrator name and Password.**

The system administrator's user name is `admin` by default. You must use a system administrator account, and not a limited administrator account or domain administrator account.

– Check **Replicate client packages and LiveUpdate content between the local site and this partner site** (Optional).

If you don't check this option now, you can check it later.

5. If a warning message about accepting the certificate appears, click **Yes**.

6. In the site information pane, accept or change the default values, and then click **Next**.

7. In the database choice pane, click either the **Default SQL Server Express database** or **Microsoft SQL Server database**, and then click **Next**.

Symantec recommends that the site with which you replicate uses the same type of database, but it is not required. For 14.3 MPx and earlier, the default database is the **Default Embedded database**.

Complete the installation based on the database that you choose.

8. In the **Run LiveUpdate** pane, click **Next**.

Optionally add the partner information.

9. Optionally accept the data collection feature, and then click **Next**.

The database gets created. This step takes some time.

The Symantec Endpoint Protection Manager launches.

Change the schedule, if necessary. See:

[Changing the replication frequency and content](#)

More information

- [Setting up sites and replication](#)
- [What are sites and how does replication work?](#)
- [Deciding whether or not to set up multiple sites and replication](#)
- [Preventing replication during an upgrade](#)

Changing the replication frequency and content

By default, replication is scheduled to occur automatically after you install the second site and management server. Replication occurs according to the default schedule as part of installing the second management server. However, you may need to change the frequency based on how long replication takes. You can change the frequency on either the local site or the new site, but Symantec recommends that you configure replication on the new site first. The schedule on both sites is the same the next time the two sites replicate. The site with the smaller ID number initiates the scheduled replication. Whichever site is configured as the new replication partner always has its database overwritten by the database from the local site that the new site points to.

Both sites automatically share groups and policies. You can choose whether to replicate logs, client installation packages, or LiveUpdate content based on the amount of disk space that is available.

The time that it takes to replicate depends on the size of the database as well as network connection between the sites. First, test a replication cycle to see how long it takes. You should schedule your replication based on that time period, and make sure that the time when the management servers duplicate data does not overlap. Both the client packages and LiveUpdate content can include a large volume of data. The data in a client package might be as large as 5 GB. The client installation packages may require as much as 500 MB of disk space. If you plan to replicate logs, make sure that you have sufficient disk space for the additional logs on all the replication partner servers.

After the initial, full database replication, subsequent replications are fairly small, if you only replicate policies, clients, and groups, and not logs. Make sure that the management servers have enough available disk space to replicate based on the frequency and content.

To change the replication frequency and schedule

1. In the console, click **Admin > Servers**.
2. Under **Servers > Local Site**, expand **Replication Partners**, and select the site you want to replicate with.
3. Under **Tasks**, click **Edit Replication Partner Properties**.
4. Choose the content you want to replicate.
5. To change the schedule, do one of the following tasks:
 - Check **Auto-replicate** to let the management server choose when to replicate the data.
This option causes frequent and automatic replication to occur between two sites, about every 2 hours.
 - Check **Replicate on a schedule** to set up a custom schedule.
6. Click **OK**.

More information

[Replication considerations and best practices](#)

Replicating data immediately

Replication normally occurs according to the default schedule when you set up an additional site. You might want replication to occur immediately. The site with the smaller ID number initiates the scheduled replication.

If you use the Microsoft SQL Server database with more than one server, you can only initiate replication from the first server at that site.

To replicate data immediately

1. In the console, click **Admin > Servers**.
2. Under **Servers > Local Site**, expand **Replication Partners** and select the site.
3. Under **Tasks**, click **Replicate Now**.
4. Click **Yes**, and then **OK**.

More information

- [Changing the replication frequency and content](#)
- [Setting up sites and replication](#)

Deleting sites

Deleting a replication partner disconnects the partnership in Symantec Endpoint Protection Manager, but does not uninstall the management server software or delete the second site.

If you remove the management server at a remote site, you need to manually delete it from all sites. Uninstalling the software from one management server console does not make the icon disappear from the **Servers** pane on other consoles. See:

[Disabling replication and restoring replication before and after an upgrade](#)

To delete a site

1. In the console, click **Admin > Servers > Local Site**, expand **Replication Partners**, right-click the replication partner, and click **Delete Replication Partner**.
2. Under **Remote Sites**, right-click the site and click **Delete Remote Site**.
3. Click **Yes**.

More information

[Setting up sites and replication](#)

Disaster recovery best practices for Endpoint Protection

To prepare for recovery after a hardware failure or database corruption, you should back up the information that is collected after you install Symantec Endpoint Protection Manager.

Refer to the following topics for more information:

Preparing for disaster recovery

Follow these steps to prepare.

Table 192: High-level steps to prepare for disaster recovery

Step	Description
Step 1: Back up the database	Back up the database regularly, preferably weekly. By default, the database backup folder is saved to the following default location: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup The backup file is called date_timestamp.zip. For more information, see: Backing up the database and logs
Step 2: Back up the most recent disaster recovery file	The recovery file includes the encryption password, keystore files domain ID, certificate files, license files, and port numbers. By default, the file is located in the following directory: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_timestamp.zip The recovery file only stores the default domain ID. If you have multiple domains, the recovery file does not store that information. If you need to perform disaster recovery, you must re-add the domains. See: Adding a domain If you have multiple zip files, back up the most recent file only.
Step 3: Update or back up the server certificate (optional)	If you update the self-signed certificate to a different certificate type, the management server creates a new recovery file. Because the recovery file has a timestamp, you can tell which file is the latest one. See: • Updating or restoring a server certificate • Backing up a server certificate
Step 4: Save the IP address and host name of the management server to a text file (optional)	If you have a catastrophic hardware failure, you must reinstall the management server using the IP address and host name of the original management server. Add the IP address and host name to a text file, such as: Backup.txt.
Step 5: Store the backup data in a secure location off-site	Copy the files you backed up in the previous steps to another computer

Performing disaster recovery

The following table lists the steps to recover your Symantec Endpoint Protection environment in the event of hardware failure or database corruption.

Before you follow these steps, make sure that you made backups and recovery files.

Table 193: Process for performing disaster recovery

Step	Action
Step 1: Reinstall Symantec Endpoint Protection Manager using a disaster recovery file.	By reinstalling the management server, you can recover the files that were saved after initial installation. See: Reinstalling or reconfiguring Symantec Endpoint Protection Manager If you reinstall Symantec Endpoint Protection Manager on a different computer and without using the disaster recovery file, you must generate a new server certificate. See: Generating a new server certificate
Step 2: Restore the database.	You can restore the database with or without a database backup. See: Restoring the database
Step 3: Re-enable Federal Information Processing Standards (FIPS) 140-2 compliance. (optional)	If you use a FIPS-compliant version of Symantec Endpoint Protection and have FIPS compliance enabled, after you recover Symantec Endpoint Protection Manager, you must reenable FIPS compliance. This setting is not stored in the disaster recovery file.

More information

- [Backing up your license files](#)
- [Exporting and importing server settings](#)
- [Disaster recovery best practices for Endpoint Protection](#)

Backing up the database and logs

Symantec recommends that you back up the database at least weekly. You should store the backup file on another computer.

By default, the backup file is saved in the following folder: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\data\backup.

The backups are placed in a .zip file. By default, the backup database file is named date_timestamp.zip, the date on which the backup occurs.

NOTE

Avoid saving the backup file in the product installation directory. Otherwise, the backup file is removed when the product is uninstalled.

Log data is not backed up unless you configure Symantec Endpoint Protection Manager to back it up. If you do not back up the logs, then only your log configuration options are saved during a backup. You can use the backup to restore your database, but the logs in the database are empty of data when they are restored.

You can keep up to 10 versions of site backups. You should ensure that you have adequate disk space to keep all your data if you choose to keep multiple versions.

You can check the System log as well as the backup folder for the status during and after the backup.

You can back up the database immediately, or schedule the backup to occur automatically.

NOTE

The Microsoft SQL Server Express database has a 10 GB limit. To back up the database, you cannot have more than 10 GB in the database and you must have at least 10 GB of available disk space.

For more information, see:

- [Scheduling automatic database backups](#)
- [Disaster recovery best practices for Endpoint Protection](#)

To back up the database and logs

1. On the computer that runs Symantec Endpoint Protection Manager, on the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.
2. In the **Database Back Up and Restore** dialog box, click **Back Up**.
3. In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.
4. Click **OK**.
5. When the database backup completes, click **Exit**.
6. Copy the backup database file to another computer.

To back up the database and logs from within the console

1. On the console, click **Admin > Servers**.
2. Under **Servers**, click **Local Site (My Site) > SQLEXPRESSSYMC** (as of 14.3 RU1) or **localhost**.
3. Under **Tasks**, click **Back Up Database Now**.
4. In the **Back Up Database** dialog box, optionally check **Backup logs**, and then click **Yes**.
5. Click **OK**.
6. Click **Close**.

Backing up a server certificate

In case the computer on which the management server is installed gets corrupted, you should back up the private key and the certificate.

The JKS Keystore file is backed up during the initial installation. A file that is called `server_timestamp.xml` is also backed up. The JKS Keystore file includes the server's private and public key pair and the self-signed certificate.

To back up a server certificate

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, click the management server whose server certificate you want to back up.
3. Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
4. In the **Manage Server Certificate** panel, click **Back up the server certificate** and then click **Next**.
5. In the **Back Up Server Certificate** panel, click **Browse** to specify a backup folder, and then click **Open**.

NOTE

You back up the management server certificate into the same folder.

6. In the **Backup Server Certificate** panel, click **Next**.
7. Click **Finish**.

More information

- [About server certificates](#)
- [Generating a new server certificate](#)

Reinstalling or reconfiguring Symantec Endpoint Protection Manager

If you need to reinstall or reconfigure the management server, you can import all your settings by using a disaster recovery file. You can reinstall the software on the same computer, in the same installation directory. Symantec Endpoint Protection Manager creates a recovery file during installation. You can also use this procedure to reconfigure the existing site, or to install an additional site for replication.

See also:

[Disaster recovery best practices for Endpoint Protection](#)

To reinstall the management server

1. Uninstall the existing management server.
2. Install the server from the installation file.

[Installing Symantec Endpoint Protection Manager](#)

3. In the **Welcome** panel, make sure that the **Use a recovery file to restore communication with previously deployed clients** option is checked, and then click **Next**.

By default, the recovery file is located in: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Server Private Key Backup. The recovery file reconnects your clients to the Symantec Endpoint Protection Manager.

4. Follow the instructions in each panel. The default settings work for most cases. If the reinstalled server connects to an existing database, you change the database settings to those of the existing database.

You can also restore the database if necessary. However, if the Symantec Endpoint Protection Manager database resides on another computer or is otherwise not affected, you do not need to restore your database.

[Restoring the database](#)

To reconfigure the management server

1. Click **Start > All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Management Server Configuration Wizard**.

2. Select one of the following options:

- To reconfigure the management server on the existing site, click **Reconfigure the management server**.
- To reconfigure the management server to replicate data with an existing site, click **Reconfigure the management server to replicate with a different site**.

This option reconfigures the locally installed management server to create a new site and to replicate the data with another existing site in your network. Also, if you have two non-replicating sites, use this option to convert one of the sites into a site that replicates with the second site.

NOTE

If you leave **Use a recovery file to restore communication with previously deployed clients** checked, the installation proceeds. However, it ignores the default domain ID in the recovery file and uses the domain ID of the replication partner. After reconfiguration completes, existing clients may fail to connect due to the change in domain ID.

3. Follow the instructions in each panel.

More information

[Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)

Generating a new server certificate

You generate a new server certificate for Symantec Endpoint Protection Manager if the IP address or host name of the server changes, or if your private key was compromised.

By default, client-server communication depends on verifying the server certificate. If you generate a new server certificate, this verification fails and communication is interrupted. See:

[Updating the server certificate on the management server without breaking communications with the client](#)

To generate a new server certificate

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, click the management server.
3. Under **Tasks**, click **Manage Server Certificate**, and then click **Next**.
4. In the **Manage Server Certificate** panel, click **Generate new server certificate**. Make sure that **Generate new Keys** is checked, and then click **Next**.

Generate new Keys generates a new certificate with a new key pair (public and private keys). If you uncheck this option, the new certificate uses the same key pair as before, which lowers the Symantec Endpoint Protection Manager server security profile in the case of a compromised key pair.

5. Click **Yes**, and then click **Next**.
6. You must restart the following services to use the new certificate:
 - The Symantec Endpoint Protection Manager service
 - The Symantec Endpoint Protection Manager Webserver service
 - The Symantec Endpoint Protection Manager API service

For more information, see:

- [Stopping and starting the management server service](#)
- [Stopping and starting the Apache Web server](#)

The next time you log on to Symantec Endpoint Protection Manager, you are asked to trust the new certificate.

More information

- [Accepting the self-signed server certificate for Symantec Endpoint Protection Manager](#)
- [Logging on to the Symantec Endpoint Protection Manager console](#)

Restoring the database

If the database gets corrupted or you need to perform disaster recovery, you can restore the database. To restore the database, you must first have backed it up. See:

[Backing up the database and logs](#)

NOTE

You must restore the database using the same version of Symantec Endpoint Protection Manager that you used to back up the database. You can restore the database on the same computer on which it was installed originally or on a different computer.

The database restore might take several minutes to complete.

To restore the database with a database backup:

1. Stop the management server service. See:
[Stopping and starting the management server service](#)
2. On the **Start** menu, click **All Programs > Symantec Endpoint Protection Manager > Symantec Endpoint Protection Manager Tools > Database Back Up and Restore**.
3. In the **Database Back Up and Restore** dialog box, click **Restore**.
4. Click **Yes** to confirm the database restoration.

-
5. In the **Restore Site** dialog box, select the backup database file, and then click **OK**.
 6. Locate the copy of the backup database file that you made when you backed up the database. By default, the backup database file is named `date_timestamp.zip`.
 7. Click **OK**.
 8. Click **Exit**.
 9. Restart the management server service.

To restore the database without a database backup:

You may need to restore the database without a database backup in the following cases:

- You tried and cannot reset your administrator password. See:
[Resetting a forgotten Symantec Endpoint Protection Manager password](#)
 - You did not make a database backup and the database is corrupted.
 - You need to restore the database as new without reinstalling SEPM. (Skip to step 3)
1. Back up the policy files.
You import the exported policy files after you reinstall the database.
 2. If you have multiple domains, create a text file named `SEPBackup.txt` and add any domain IDs. (Optional)
To save the management server information, add the IP address and host name of the management server to the file.
 3. Stop the management server service. See:
[Stopping and starting the management server service](#)
 4. Reconfigure the management server using the Management Server Configuration Wizard and the recovery file. See:
[Reinstalling or reconfiguring Symantec Endpoint Protection Manager](#)
 5. On the reconfigured Symantec Endpoint Protection Manager, in the following file:
`SEPM_Install/tomcat/etc/conf.properties`
The default for `SEPM_Install` is `C:/Program files (x86)/Symantec/Symantec Endpoint Protection Manager`.
Change:
`scm.agent.groupcreation=false` to `scm.agent.groupcreation=true`
This edit enables the automatic creation of client groups. Otherwise, the clients to reappear in the default group as they check in.
Clients can communicate with Symantec Endpoint Protection Manager, but only re-appear in the console only after their next check-in.

Virtual environments with Symantec Endpoint Protection

Configure the clients to run on virtual machines.

Symantec Endpoint Protection provides the Shared Insight Cache and Virtual Image Exception features for virtual infrastructures, which you can enable to improve performance. You need to perform some additional installation and configuration tasks to enable these features.

Table 194: Virtual infrastructure features and their use

Feature and use	Description
Use Shared Insight Cache to skip the scanning of files that are known to be clean.	Shared Insight Cache keeps track of the files that are known to be clean. Shared Insight Cache can reduce the scan load by eliminating the need to rescan those files. You can set up the following types of Shared Insight Cache: • A network-based Shared Insight Cache Virtual clients that use any kind of virtual infrastructure can use a network-based Shared Insight Cache to reduce scan loads. For more information, see: • About Shared Insight Cache • What do I need to do to use a network-based Shared Insight Cache?
Use the Virtual Image Exception tool so that clients can skip the scanning of base image files.	The Virtual Image Exception tool lets you mark base image files as safe so that scans skip those files to reduce scan loads. The Virtual Image Exception tool runs in a virtual environment only. See: About the Virtual Image Exception tool
Configure the non-persistent virtual desktop infrastructures feature.	Symantec Endpoint Protection clients have a configuration setting to indicate that they are non-persistent virtual clients. You can configure a separate aging period for the offline GVMs in non-persistent virtual desktop infrastructures. Symantec Endpoint Protection Manager removes non-persistent GVM clients that have been offline longer than the specified time period. See: • Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures • Purging obsolete non-persistent VDI clients to free up licenses

The protection technologies in Symantec Endpoint Protection Manager and Symantec Endpoint Protection typically function the same way in virtual infrastructures as they do in physical infrastructures. You can install, configure, and use Symantec Endpoint Protection Manager and Symantec Endpoint Protection clients in virtual infrastructures in the same way as in physical infrastructures.

About Shared Insight Cache

Shared Insight Cache use improves performance in virtual infrastructures. Files that Symantec Endpoint Protection clients have determined to be clean are added to the cache. The subsequent scans that use the same virus definitions version can ignore the files that are in the Shared Insight Cache. Shared Insight Cache is used only for scheduled and manual scans.

The network-based Shared Insight Cache runs as a Web service that is independent of the Symantec Endpoint Protection client. Shared Insight Cache uses a voting system. After a client uses the latest content to scan a file and determines that it is clean, the client submits a vote to the cache. If the file is not clean, the client does not submit a vote. When the vote count for a file is greater than or equal to the vote count threshold, then Shared Insight Cache considers the file clean. When another client subsequently needs to scan the same file, that client first queries Shared Insight Cache. If the file is marked clean for their current content, then the client does not scan that file.

When a client sends a vote to Shared Insight Cache, the cache checks the version of content that the client used to scan the file. If the client does not have the latest content, Shared Insight Cache ignores the vote. If newer content is available, the newer content becomes the latest known content and Shared Insight sets the vote count back to one.

To keep the cache size manageable, Shared Insight Cache uses a pruning algorithm. The algorithm removes the oldest cache entries, which are those with the oldest timestamp, first. This algorithm ensures that the cache size does not exceed the memory usage threshold.

More information

- [What do I need to do to use a network-based Shared Insight Cache?](#)
- [Customizing Shared Insight Cache settings](#)
- [Using Symantec Endpoint Protection in virtual infrastructures](#)

About the Virtual Image Exception tool

The Virtual Image Exception tool lets clients bypass the scanning of the base image files for threats. This feature reduces the resource load on disk I/O and on the CPU.

Symantec Endpoint Protection supports the use of Virtual Image Exceptions for both managed clients and unmanaged clients.

NOTE

Symantec does not support the use of the Virtual Image Exception tool in physical environments.

More information

- [Using the Virtual Image Exception tool on a base image](#)
- [Using Symantec Endpoint Protection in virtual infrastructures](#)

What do I need to do to use a network-based Shared Insight Cache?

You can use a network-based Shared Insight Cache to improve scan performance.

Table 195: Tasks to install and use a network-based Shared Insight Cache

Step	Task
Step 1: Install Shared Insight Cache.	• System requirements for implementing a network-based Shared Insight Cache • Installing and uninstalling a network-based Shared Insight Cache
Step 2: In the Virus and Spyware policy in Symantec Endpoint Protection Manager, enable your virtual clients to use Shared Insight Cache	Enabling the use of a network-based Shared Insight Cache

After you have installed a Shared Insight Cache, you can optionally do the following tasks:

- Customize any of the service, cache, or log settings for Shared Insight Cache. See: [Customizing Shared Insight Cache settings](#)
- View related events in the log. See: [Viewing network-based Shared Insight Cache log events](#)
- Use the Windows Performance Manager to monitor its performance. See: [Monitoring network-based Shared Insight Cache performance counters](#)

System requirements for implementing a network-based Shared Insight Cache

The network-based Shared Insight Cache server is designed to run on a standalone physical or virtual machine. Shared Insight Cache should not be installed to a system running other database applications or high-availability server applications, such as Symantec Endpoint Protection Manager or Microsoft SQL Server.

The following table describes the minimum system requirements that a virtual infrastructure needs to run Shared Insight Cache.

Table 196: Network-based Shared Insight Cache system requirements

Requirement	Description
Software	• Windows Server 2008 and later • Windows Server 2012 and Windows Server 2012 R2 • Windows Server 2016 (As of 14.2 MP1) • Windows Server 2019 (As of 14.2 MP1) • .NET Framework 4
CPU	Shared Insight Cache must be installed on a dedicated server or a virtual machine.
Memory	2 GB minimum
Available disk space	100 MB minimum

More information

- [About Shared Insight Cache](#)
- [Installing and uninstalling a network-based Shared Insight Cache](#)

Installing and uninstalling a network-based Shared Insight Cache

Before you install the network-based Shared Insight Cache, ensure that you have met all the system requirements and that you are logged on as a Windows administrator. You install and run the Shared Insight Cache on a standalone physical or virtual machine.

NOTE

You should not use DBCS or high-ASCII characters in the host name of the server on which you install a Shared Insight Cache. You should also refrain from using DBCS or high-ASCII characters in the user name that you use to access it. These characters cause the Shared Insight Cache service to fail to start.

For more information, see:

[System requirements for implementing a network-based Shared Insight Cache](#)

To install a network-based Shared Insight Cache

1. On the Symantec Endpoint Protection installation file, navigate to the `Tools/Virtualization/SharedInsightCache` folder.
2. Double-click the following file to launch the installation program:
`SharedInsightCacheInstallation.msi`

NOTE

You can type the following command instead, to launch the same installation program:

```
msiexec /i SharedInsightCacheInstallation.msi
```

3. In the **Shared Insight Cache Setup** wizard pane, click **Next**.
4. Read through the Symantec Software license agreement, check **I accept the terms of the License Agreement**, and then click **Next**.
5. On the **Destination Folder** pane, do one of the following tasks:
 - Click **Next** to accept the default location for Shared Insight Cache.
 - Click **Change**, browse to and select a different destination folder, click **OK**, and then click **Next**.
6. On the **Shared Insight Cache Settings** pane, specify the following Shared Insight Cache settings:

Cache Usage (% of Physical Memory)	The maximum size of the cache. When the cache exceeds this threshold, Shared Insight Cache prunes the cache size.
Listening Port	The port on which the server listens.
Status Listening Port	The port that the server uses to communicate status about the server.

7. Click **Install**.
8. When the installation has completed, click **Finish**.

For more information, see:

[Customizing Shared Insight Cache settings](#)

Uninstalling Shared Insight Cache has the same effect as stopping the Shared Insight Cache service. If you are uncertain as to whether you want to permanently uninstall Shared Insight Cache, you can stop the service instead. See:

[About stopping and starting the network-based Shared Insight Cache service](#)

NOTE

To uninstall the Shared Insight Cache, use the appropriate Windows control panel, such as Add or Remove Programs. You must have Windows administrator rights to uninstall Shared Insight Cache.

If you uninstall Shared Insight Cache, you may also want to disable the Shared Insight Cache in Symantec Endpoint Protection Manager. Disabling Shared Insight Cache prevents the Windows Event log from receiving notifications each time clients cannot contact the cache.

Enabling the use of a network-based Shared Insight Cache

For communication with Symantec Endpoint Protection clients over the network, by default Shared Insight Cache uses no authentication and no SSL. If you change Shared Insight Cache settings to Basic authentication with SSL or Basic authentication with no SSL, you must specify a user name and password that can access Shared Insight Cache. See:

[Customizing Shared Insight Cache settings](#)

To enable the use of a network-based Shared Insight Cache

-
1. In the Symantec Endpoint Protection Manager console, open the appropriate Virus and Spyware Protection policy and click **Miscellaneous**.
 2. On the **Shared Insight Cache** tab, check **Shared Insight Cache using Network**.
 3. Click **Require SSL** if you enabled SSL authentication in the configuration file.
 4. In the **Hostname** box, type the host name of the host on which you installed Shared Insight Cache.
 5. In the **Port** box, type the port number of Shared Insight Cache.
 6. Optionally, if you configured authentication for Shared Insight Cache:
 - In the **Username** box, type the user name.
 - Optionally, click **Change Password** to change the default password (null) to the password that you created for authentication.
Leave these fields empty if you do not want to use a password.
 7. Click **OK**.

More information

[What do I need to do to use a network-based Shared Insight Cache?](#)

Customizing Shared Insight Cache settings

After you install Shared Insight Cache, you can customize its settings in the configuration file.

The configuration file is an XML file that follows .NET Framework application configuration standards. Shared Insight Cache does not start if there is an invalid configuration, such as invalid XML, incorrect value types, or missing required values.

For more information, see:

[Configuration Editor Tool \(SvcConfigEditor.exe\)](#)

The following table describes the options that you can configure.

Table 197: Shared Insight Cache configuration options

Option and default value	Description and comments
Cache Service Listening Port The default value is 9005.	Port on which the service listens. The listening port is used by clients to submit scan results for files and to make requests to determine if the client should scan a file. If the range for the port is not between 0 - 65535, the service does not start. The service does not start if it cannot listen on the specified port. <pre><endpoint address="http://localhost:9005/1"</pre> By default, the Shared Insight Cache server listens on all IP addresses. To configure the listening IP addresses for HTTP or HTTPS services, you must use Netsh.exe. The Shared Insight Cache server listens on the IP addresses that you specified in the IP Listen List modified by those tools. Netsh.exe is included with Windows Server 2008. For more information, see: Configuring HTTP and HTTPS
Status Service Listening Port The default value is 9006.	Port the server uses to communicate status about the server. The status listening port uses a SOAP-based interface on the port specified in the configuration section. This interface provides a mechanism by which an administrator can query information and status about the Cache Server. The service does not start if the range is not between 0 - 65535. The service does not start if it cannot listen on the specified port.
Vote Count The default value is 1.	Number of the clients that must verify that the file is clean before Shared Insight Cache uses the results. The value must be less than or equal to 15. If the value is greater than 15, the server uses the default value. <pre><cache.configuration vote.count="1" /></pre>
Prune Size The default value is 10.	Percentage of memory usage to remove from the cache when the cache hits the memory usage limit. The value must be between 10 and 100. If the value is not between 10 and 100, the server uses the default value. Note: Symantec recommends that you keep the default prune size. <pre><prune.size="10" /></pre>
Memory Usage The default value is 50.	Percentage of size of the cache before Shared Insight Cache starts pruning the cache. Must be greater than or equal to 10. <pre><mem.usage="50" /></pre>
Log File The default value is install_folder\CacheServer.log	A file for the Shared Insight Cache log. <pre><filevalue="CacheServer.log" /></pre>
Log Level The default value is ERROR.	ALL DEBUG INFO WARN ERROR FATAL OFF A value of OFF indicates that Shared Insight Cache does not log any messages. <pre><level value="ERROR" /></pre> For more information, see: Viewing network-based Shared Insight Cache log events

Option and default value	Description and comments
Log Size The default value is 10000.	Size of the log (in bytes) until Shared Insight Cache rolls the log over. <code><maximumFileSizevalue="10000" /></code>
Log Backups The default value is 1.	Number of rolled over logs to keep before the oldest log is deleted. A value of 0 indicates that Shared Insight Cache retains no backups. A negative value indicates that Shared Insight Cache retains an unlimited number of backups. <code><maxSizeRollBackupsvalue="1" /></code>
Enable SSL Enable authentication	By default, Shared Insight Cache is set up with no authentication and no SSL. It can be changed to Basic authentication with SSL, no authentication with SSL, or Basic authentication with no SSL. <pre> <webHttpBinding> <bindingname="CacheServerBinding"> <!-- Uncomment the appropriate section to get the desired security. If enabling ssl modify the uri to use https. A cert will also have to be installed and registered for the ip/port. --> <!-- Basic authentication with SSL.--> <security mode="Transport"> <transport clientCredentialType="Basic"/> </security--> <!-- No authentication with SSL.--> <security mode="Transport"> <transport clientCredentialType="None"/> </security--> <!-- Basic authentication with no SSL.--> <security mode="TransportCredentialOnly"> <transport clientCredentialType="Basic"/> </security--> <!-- No authentication with no SSL. DEFAULT --> <securitymode="None"> <transportclientCredentialType="Basic"/> </security> </binding> </webHttpBinding> </pre> For more information, see: Enabling the use of a network-based Shared Insight Cache

To customize Shared Insight Cache settings

1. Navigate to and open the following file:

C:\Program Files (x86)\Symantec\Shared Insight Cache
\SharedInsightCacheInstallation.exe.config

This file path may vary for legacy installations.

-
2. Make the modifications as needed.
 3. Save your changes and close the file.
 4. Restart the Shared Insight Cache service.

You must restart the Shared Insight Cache service for changes to all configuration settings except the log level to take effect. See:

[About stopping and starting the network-based Shared Insight Cache service](#)

More information

[What do I need to do to use a network-based Shared Insight Cache?](#)

About stopping and starting the network-based Shared Insight Cache service

You may need to stop the Shared Insight Cache service temporarily to troubleshoot an issue. After you have resolved the issue, you can restart the service. You can start and stop the service from the Service Control Manager.

Uninstalling Shared Insight Cache has the same effect as stopping the Shared Insight Cache service. If you are uncertain as to whether you want to permanently uninstall Shared Insight Cache, you can stop the service instead.

You must have Windows administrator rights to stop and start the Shared Insight Cache service. See:

[Troubleshooting issues with Shared Insight Cache](#)

Viewing network-based Shared Insight Cache log events

You can view the Shared Insight Cache log file to see any events that Shared Insight Cache creates. The log file is located in the installation folder and is named `CacheServer.log`.

Shared Insight Cache prints logs in the following format:

```
[ ] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message [-]%newline
```

For example:

```
[ ] 4 | 12/15/2010 10:51:37 | INFO | CacheServerService.Service | Started service [-]
```

Modify the configuration file to specify the log level that you want to use for network-based Shared Insight Cache.

The following table describes the levels that you can set.

Table 198: Network-based Shared Insight Cache log levels

Log level	Description
OFF	OFF indicates that no incidents are logged.
FATAL	FATAL messages require you to take action. These messages are the errors that cause Shared Insight Cache to stop. For example, a FATAL message may indicate that the server IP address is not available, which means that Shared Insight Cache cannot run.
ERROR	ERROR messages require you to take action, but the process continues to run. They are errors in the system that cause Shared Insight Cache to fail or lose functionality. You also receive all log entries for FATAL messages. This level is the default logging level.

Log level	Description
WARN	WARN messages indicate Shared Insight Cache behavior that may be undesirable, but do not cause it to fail. You also receive all log entries for FATAL messages and ERROR messages.
INFO	INFO messages describe the general actions of or give information about Shared Insight Cache. They may indicate the state of the system and help validate behavior or track down issues. However, alone they are not intended to report actionable items. For example, an information message may indicate that cache pruning is complete. The message does not detail a problem. It only logs behavior. You also receive all log entries for FATAL messages, ERROR messages, and WARN messages.
DEBUG ALL	DEBUG and ALL log level messages produce the same results. These log levels are intended for Support to troubleshoot problems with Shared Insight Cache. You also receive all log entries for all other log levels.

Increase the log level only when you need to troubleshoot issues with Shared Insight Cache. When you increase the log level, you begin to significantly increase the size of the log file. When you resolve the issue, return to the default log level of ERROR.

Go to the following location:

Installation folder/CacheServer.log

More information

[Customizing Shared Insight Cache settings](#)

Monitoring network-based Shared Insight Cache performance counters

You can view network-based Shared Insight Cache statistics in the Windows Performance Monitor. The Shared Insight Cache service must be running to view its performance counters.

Table 199: Shared Insight Cache statistics

Statistic	Description
The number of items in the cache	This number represents the current number of items in the cache.
The number of items in the cache that have been voted clean	This number represents the current number of items in the cache, which have been voted clean.
Number of cache requests	The number of cache requests that have been made to the Shared Insight Cache service. This number includes only the number of valid requests that received a 200 response. This counter does not persist across restarts of the service.
Number of update requests	The number of update requests that have been made to the service. This number is only the valid requests that received a 200 response. This counter does not persist across restarts of the service.

To monitor network-based Shared Insight Cache performance counters

1. At the command prompt, type the following command:

```
perfmon
```

2. In the **Performance** window, right-click the graph.
3. Select **Add Counters**.
4. In the **Performance object** drop-down list, select **Shared Insight Cache**.
5. Select the counters that you want to view, and click **Add**.
6. Click **Close**.

The Shared Insight Cache counters that you selected appear in the Performance graph.

For more information about using the Windows performance monitor, see your Windows documentation.

More information

- [Troubleshooting issues with Shared Insight Cache](#)
- [What do I need to do to use a network-based Shared Insight Cache?](#)

Troubleshooting issues with Shared Insight Cache

The following table provides suggestions for how to troubleshoot issues with Shared Insight Cache.

Table 200: Troubleshooting Shared Insight Cache

Issue	Explanation/Resolution
Experiencing problems with the cache results	Restart the service. See: About stopping and starting the network-based Shared Insight Cache service
Shared Insight Cache returns a "no result" response	Shared Insight Cache returns a no result response when it fails to successfully perform a cache lookup. If the client requests a cache lookup, a no result means that the file must be scanned. Note: Shared Insight Cache returns a success response even when it fails to successfully perform a cache update. The reason is because the client is not required to perform a different action when a failure occurs.
Suspected issues with HTTP traffic	View the HTTP traffic error log. The HTTP traffic errors are logged in the following location: %Windir%\System32\Logfiles\HTTPERR

More information

- [Viewing network-based Shared Insight Cache log events](#)
- [Monitoring network-based Shared Insight Cache performance counters](#)

Using the Virtual Image Exception tool on a base image

You can use the Virtual Image Exception tool on a base image before you build out your virtual machines. The Virtual Image Exception tool lets your clients bypass the scanning of base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in your virtual desktop infrastructure.

Symantec Endpoint Protection supports the use of the Virtual Image Exception tool for managed clients and unmanaged clients

NOTE

You cannot use the Virtual Image Exception tool in a non-virtual environment.

Table 201: Process for using the Virtual Image Exception tool on a base image

Step	Action
Step 1	On the base image, perform a full scan all of the files to ensure that the files are clean. If the Symantec Endpoint Protection client quarantines infected files, you must repair or delete the quarantined files to remove them from quarantine.
Step 2	Ensure that the client's quarantine is empty.
Step 3	Run the Virtual Image Exception tool from the command line to mark the base image files. See: Running the Virtual Image Exception tool vietool
Step 4	Enable the feature in Symantec Endpoint Protection Manager so that your clients know to look for and bypass the marked files when a scan runs. See: Configuring Symantec Endpoint Protection to bypass the scanning of base image files
Step 5	Remove the Virtual Image Exception tool from the base image.

The Virtual Image Exception tool supports fixed, local drives. It works with the files that conform to the New Technology File System (NTFS) standard.

More information

[System requirements for the Virtual Image Exception tool](#)

System requirements for the Virtual Image Exception tool

The Virtual Image Exception tool is supported for use on VMware ESX, Microsoft Hyper-V, and Citrix XenDesktop platforms.

The client must be installed in one of the supported virtual environments.

WARNING

The client must be the same version as the Virtual Image Exception tool.

For the most up-to-date information about requirements and supported platforms, see the following webpage:

[Release notes, new fixes, and system requirements for all versions of Endpoint Protection](#)

More information

[Using the Virtual Image Exception tool on a base image](#)

Running the Virtual Image Exception tool

Before you run the Virtual Image Exception tool, ensure that you have met all of the system requirements.

WARNING

The client must be the same version as the Virtual Image Exception tool.

For more information, see:

[System requirements for the Virtual Image Exception tool](#)

To run the Virtual Image Exception tool

1. From the Symantec Endpoint Protection Tools folder of the installation file, download the following file to the base image:

```
/Virtualization/VirtualImageException/vietool.exe
```

-
2. Open a command prompt with administrative privileges.
 3. Run the Virtual Image Exception tool with the proper arguments.

For example, type: `viectool c: --generate`

More information

[viectool](#)

Configuring Symantec Endpoint Protection to bypass the scanning of base image files

After you run the Virtual Image Exception tool on base image files, you can enable the use of Virtual Image Exceptions in Symantec Endpoint Protection Manager. Once the feature is enabled, virtual clients look for the attribute that the tool inserted. Symantec Endpoint Protection then skips the scanning of base image files that contain the attribute.

You can bypass the scanning of unchanged base image files for Auto-Protect scanning or administrator-defined scans (such as manual scans or scheduled scans).

To configure Symantec Endpoint Protection to use Virtual Image Exception to bypass the scanning of base image files

1. On the console, open the appropriate Virus and Spyware Protection policy.
2. Under **Advanced Options**, click **Miscellaneous**.
3. On the **Virtual Images** tab, check the options that you want to enable.
4. Click **OK**.

More information

[Using the Virtual Image Exception tool on a base image](#)

Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures (NPVDIs)

You can configure Symantec Endpoint Protection in a virtual environment.

Table 202: Tasks to use Symantec Endpoint Protection in non-persistent virtual desktop infrastructures

Step	Description
Step 1: Set up the base image.	You configure the Symantec Endpoint Protection client in your base image to indicate that it is a non-persistent virtual client. See: Setting up the base image for non-persistent guest virtual machines in VDIs
Step 2: In Symantec Endpoint Protection Manager, configure a separate purge interval for offline non-persistent VDI clients.	Symantec Endpoint Protection Manager removes the non-persistent GVM clients that have been offline longer than the specified time period. This feature makes it simpler to manage the GVMs in Symantec Endpoint Protection Manager. See: Purging obsolete non-persistent VDI clients to free up licenses

Setting up the base image for non-persistent guest virtual machines in non-persistent VDIs (NPVDIs)

You can set your base image up to make it simpler to use Symantec Endpoint Protection Manager to manage GVMs in non-persistent virtual desktop infrastructures.

Table 203: Tasks to set up the base image for non-persistent GVMs

Step	Description
Step 1: Install Symantec Endpoint Protection on the base image.	For more information, see: Choosing a method to install the client using the Client Deployment Wizard
Step 2: Disable Tamper Protection in the management server so that you can modify the registry.	For more information, see: Changing Tamper Protection settings
Step 3: Make sure that Symantec Endpoint Protection Manager correctly counts the number of licenses for non-persistent virtual clients.	The advantage of non-persistent clients is that offline non-persistent clients do not count toward the number of deployed licenses. Only online clients count. To mark a virtual client as a non-persistent client, you must create a registry key in the base image. For more information, see: How to manage the license count for non-persistent VDI clients
Step 4: In Symantec Endpoint Protection Manager, re-enable Tamper Protection.	For more information, see: Changing Tamper Protection settings

After you have finished setting up the base image, you can configure a separate purge interval for non-persistent clients in Symantec Endpoint Protection Manager. See:

[Purging obsolete non-persistent VDI clients to free up licenses](#)

Purging obsolete non-persistent (NPVDI) clients to free up licenses

Over time, obsolete clients can accumulate in the Symantec Endpoint Protection Manager database. Obsolete clients are those clients that have not connected to Symantec Endpoint Protection Manager for 30 days. Symantec Endpoint Protection Manager purges obsolete clients every 30 days by default.

If you do not want to wait the same number of days to purge obsolete non-persistent clients, you can configure a separate interval for them. If you do not configure a separate interval, then offline non-persistent virtual clients are purged at the same interval that obsolete physical clients are purged.

Online non-persistent clients count toward the number of deployed licenses; offline non-persistent clients do not. See:

[How to manage the license count for non-persistent VDI clients](#)

You can also filter the offline non-persistent clients out of the view on the **Clients** page.

To purge obsolete non-persistent VDI clients to free up licenses

-
1. In the Symantec Endpoint Protection Manager console, on the **Admin** page, click **Domains**.
 2. In the **Domains** tree, click the desired domain.
 3. Under **Tasks**, click **Edit Domain Properties**.
 4. On the **Edit Domain Properties > General** tab, check the **Delete non-persistent VDI clients that have not connected for specified time** check box and change the **days** value to the desired number.

The **Delete clients that have not connected for specified time** option must be checked to access the option for offline non-persistent VDI clients.
 5. Click **OK**.

More information

[Using Symantec Endpoint Protection in non-persistent virtual desktop infrastructures](#)

How to manage the license count for non-persistent virtual desktop infrastructure (NPVDI) clients

The management server counts each license for clients on physical computers, whether the computer is online or offline. For virtual clients, the management server counts the licenses of online non-persistent clients only. Offline non-persistent clients do not count. Make your virtual clients non-persistent if you have more users than you have clients.

To mark a virtual client as a non-persistent client, you must create a registry key in the base image.

To manage the license count for non-persistent VDI clients

1. After you have installed the Symantec Endpoint Protection client and disabled Tamper Protection, open the registry editor on the base image. See:

[Changing Tamper Protection settings](#)

2. Navigate to one of the following registry keys:
 - On 32-bit computers: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
 - On 64-bit computers (14.3 RU4 or earlier): HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\
 - On 64-bit computers (14.3 RU5 or later): HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
3. Create a new subkey named `Virtualization`.
4. In the **Virtualization** subkey, create a key of type `DWORD` named `IsNPVDIClient` and assign it a value of 1.

More information

- [Purging obsolete non-persistent VDI clients to free up licenses](#)
- [Setting up the base image for non-persistent guest virtual machines in VDIs](#)

viertools

viertools

viertools - Runs the Virtual Image Exception tool

SYNOPSIS

```
viertools.exe volume: --generate|clear|verify|hash [options ...]
```

DESCRIPTION

The `viertools` command marks the base image files on the volume that you specify by adding an attribute.

OPTIONS

--generate

Runs the Virtual Image Exception tool on all files on the volume specified. You cannot use this option with `--clear`.

For example: `viertools c: --generate`

--verify

Verifies that the Virtual Image Exception is set on all files on the specified volume. You cannot use this option with `--clear`.

For example: `viertools c: --verify`

--clear

Removes the Virtual Image Exception on all files on the volume specified.

For example: `viertools.exe c: --clear`

To delete a specific file: `viertools.exe c:\Users\Administrator\target.file --clear`

You can use a fully qualified path in place of the volume identifier to clear the Virtual Image Exception on a single file or the contents of a folder. Only one file name, folder name, or volume identifier per command line is allowed.

You cannot use this command with `--generate`, `--verify`, or `--hash`.

You must restart the client after you run the `--clear` command.

--hash

Generates the hash value on all files on the volume specified.

The Virtual Image Exception tool uses the hashes to exclude local files from future scans. The clients compute file hashes separately to send to the Shared Insight Cache to store scan results. You cannot use this option with `--clear`.

For example: `viertools.exe c: --generate --hash`

--volume arg

Specifies the volume the tool scans.

This option can be a file when you use the `--clear` option. You must specify the volume, and it can be specified either with the volume flag or alone. For example, with the flag `viertools.exe --volume c: --generate`, or alone `viertools.exe c: --generate`.

--verbose

Outputs to the console the maximum amount of program execution information.

--stop

Stops on the first error that the tool encounters. Otherwise the tool writes error information to the console and continues.

--help

Displays this help message.

Troubleshooting Symantec Endpoint Protection

Learn how to troubleshoot problems with Symantec Endpoint Protection.

The following table displays the most common issues that you might encounter when you install and use Symantec Endpoint Protection.

Table 204: Common issues you can troubleshoot

Task	Description
Fixing installation problems	You can download and run the Symantec Diagnostic Tool (SymDiag) to verify that your computers are ready for installation. The tool is provided from the Broadcom Support website through Help on the management server and the client. See: • Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag) • Identifying the point of failure of an installation
Fixing problems with the Microsoft SQL Server database	You can solve upgrade and installation issues with the default Microsoft SQL Server Express database or Microsoft SQL Server database. More information: • Maintaining the database • Increasing Symantec Endpoint Protection Manager available disk space before an upgrade • Increasing the Microsoft SQL Server database file size • Enabling FILESTREAM for the Microsoft SQL Server database • Configuring encrypted communication between Symantec Endpoint Protection Manager and Microsoft SQL Server • Symantec Endpoint Protection Manager has detected that the configured email server or directory server requires certificate verification to be disabled • Resolving Microsoft SQL Server database connection errors after 14.3 RU5 or later installation or upgrade
Handling virus outbreaks	You can prevent threats from attacking computers on your network. See: • Preventing and handling virus and spyware attacks on client computers • Removing viruses and security risks If a threat does attack a client computer, you can identify and respond to the threat. See: Virus removal and troubleshooting on a network
Troubleshooting content update problems	If the latest virus definitions do not update correctly on Symantec Endpoint Protection Manager or the clients, see the following article: Troubleshoot LiveUpdate and definition issues with Endpoint Protection Manager For more information, see: Symantec Endpoint Protection: LiveUpdate Troubleshooting Flowchart
Fixing communication problems	The communication channels must be open between all of the Symantec Endpoint Protection components. These channels include the following: server to client, server to database, and server and client to the content delivery component, such as LiveUpdate. See: • Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client • Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the database • Best Practices and Troubleshooting for Group Update Providers • External URLs required for Symantec Endpoint Protection (SEP)

Task	Description
Performing disaster recovery	In case of database corruption or hardware failure, you can restore the latest snapshot of the database if you have a database backup file. See: Disaster recovery best practices for Endpoint Protection
Troubleshooting reporting issues	You can solve various report and log issues. See: Troubleshooting reporting issues
Troubleshooting replication issues	For more information, see: Replication Troubleshooting Flowchart for Symantec Endpoint Protection

More information

[What are the tools included with Symantec Endpoint Protection?](#)

Troubleshooting and checking the health of the Windows client with SymDiag

SymDiag assesses the security health of Symantec products, identifies common issues, and gathers data and logs for support-assisted troubleshooting.

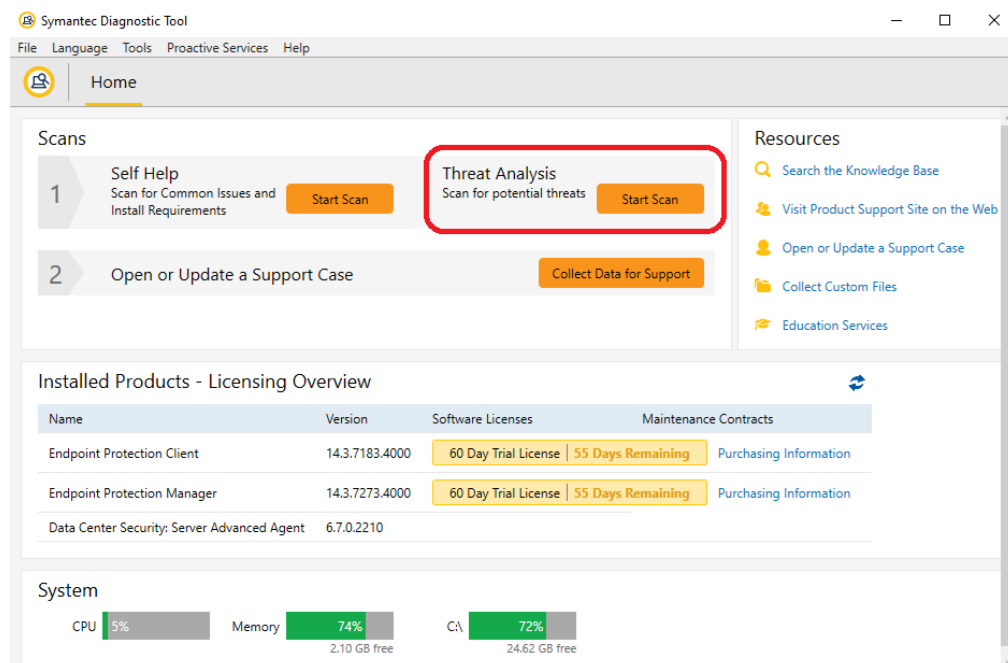
The Symantec Diagnostic (SymDiag) tool provides self-help support for Symantec product technical issues, zero-day threat analysis, best practice recommendations, and proactive services.

SymDiag:

- Lets you quickly and accurately identify known issues.
- After the tool recognizes an issue, the tool redirects you to the resources to resolve the issue yourself.
- If an issue is not resolved, the tool lets you easily submit data to Support for further diagnostics.

To download and use the SymDiag tool

1. Download the tool from the following website: [Download SymDiag to detect product issues](#)
2. Double-click the SymDiag.exe icon.
3. On the **Symantec Diagnostic Tool > Home** page, do one of the following tasks:
 - To check your security posture, under **Threat Analysis**, click **Start Scan**.



- For other self-help and troubleshooting issues, under **Self Help**, click **Start Scan**.

Enabling TLS 1.0 and 1.1 on Microsoft Windows Server 2008 R2 during an installation or upgrade

During an installation of or upgrade to the Symantec Endpoint Protection Manager (SEPM) 14.3 RU4 or later on Microsoft Windows Server 2008 R2, you may see the following message.

- Support for Microsoft Windows Server 2008 R2 has ended. To upgrade to the latest version of the Symantec Endpoint Protection Manager, you must manually enable TLS 1.1. However, TLS 1.1 is not as secure as TLS 1.2, which is supported in Windows 2012 R2 and later.

This message appears before you see the Management Server Configuration Wizard (installation) or the Management Server Upgrade Wizard (upgrade).

You must fix this issue because SEPM communicates with the clients and the database using the TLS (Transport Layer Security). Microsoft Windows Server 2008 R2 uses TLS 1.1, which is less secure than TLS 1.2. With the end of support for Windows Server 2008 R2, Microsoft disabled TLS 1.0 and 1.1.

To ensure that SEPM communicates with the clients and the database, you must do one of the following tasks:

- Upgrade to a supported version of Microsoft Windows (recommended).
- Enable TLS 1.0 and 1.1.

NOTE

14.3 RU4 is the last version of SEPM that installs or upgrades on Windows Server 2008 R2. Symantec recommends that you upgrade to a later version of Windows with TLS 1.2 support for more secure communication.

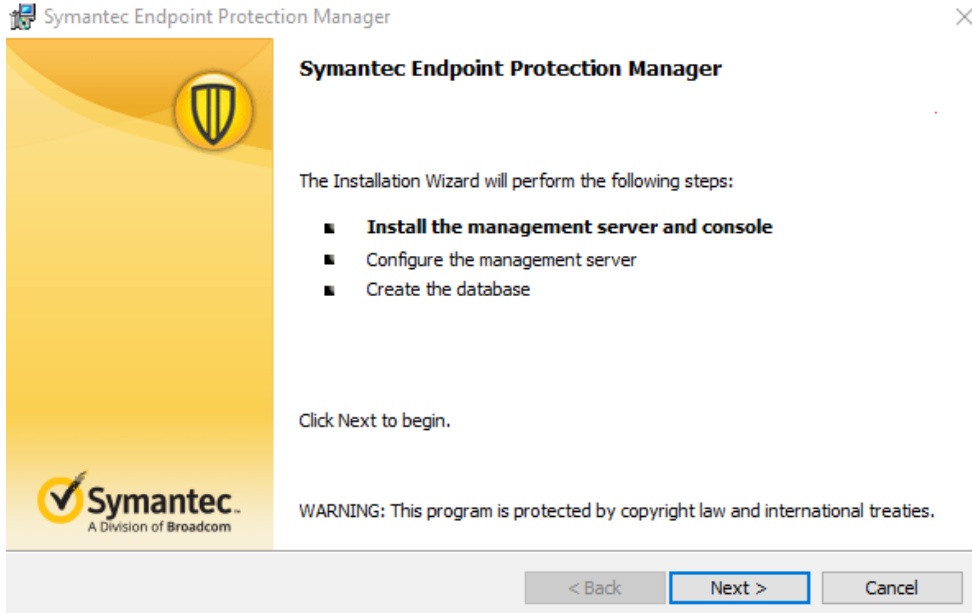
Enabling TLS 1.0 and 1.1 on Microsoft Windows Server 2008 R2

WARNING

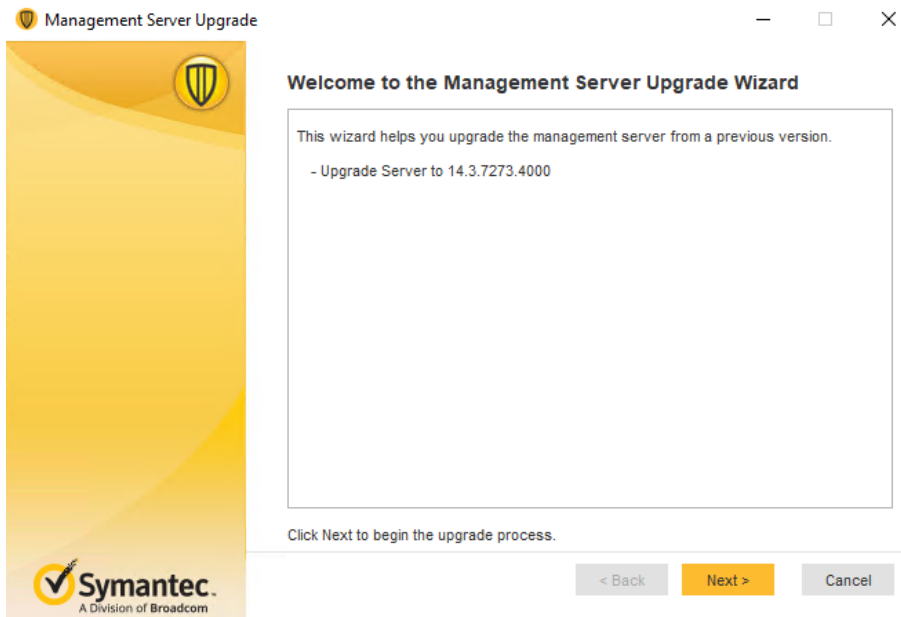
You must enable TLS 1.0 and 1.1 before the Management Server Configuration Wizard (installation) or the Management Server Upgrade Wizard (upgrade) appears or else you see failure messages.

Enable the TLS *before* you select the **Next** button:

- For a first-time installation:



- For an upgrade:



To enable TLS 1.0 and 1.1 on Windows during an installation or upgrade

- On the management server computer, open the `<SEPM_Install>\jre11\conf\java.security` file.
For example: `C:\Program Files\Symantec\Symantec Endpoint Protection Manager\jre11\conf\security\java.security`

-
2. In the `java.security` file, search for the following line: `jdk.tls.disabledAlgorithms`, which lists the disabled protocols, including TLSv1.0 and TLSv1.1.

For example:

```
jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, RC4, DES, MD5withRSA, \ DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \ include jdk.disabled.namedCurves
```

3. Remove TLSv1.0 and TLSv1.1 from the disabled protocols line.

For example:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, \ DH keySize < 1024, EC keySize < 224, 3DES_EDE_CBC, anon, NULL, \ include jdk.disabled.namedCurves
```

To enable TLS 1.0 and 1.1 on Windows after an installation or upgrade

If you do not enable TLS 1.0 and 1.1 until after the installation, relaunch the installation or upgrade wizard.

- Do one of the following tasks:
 - For a first-time installation, relaunch the Management Server Configuration wizard, double-click `Symantec \Symantec Endpoint Protection Manager\bin\sca.bat`.
 - For an upgrade, relaunch the Management Server Upgrade Wizard by double-clicking `Symantec \Symantec Endpoint Protection Manager\bin\upgrade.bat`.

Identifying the point of failure of a client installation

The Windows Installer and Push Deployment Wizard create log files that can be used to verify whether or not an installation was successful. The log files list the components that were successfully installed and provide a variety of details that are related to the installation package. You can use the log file to help identify the component or the action that caused an installation to fail. If you cannot determine the reason for the failed installation, you should retain the log file. Provide the file to Symantec Technical Support if it is requested.

NOTE

Each time the installation package is executed, the log file is overwritten.

To identify the point of failure of a client installation

1. In a text editor, open the log file that the installation generated.
2. To find failures, search for the following entry:

```
Value 3
```

The action that occurred before the line that contains this entry is most likely the action that caused the failure. The lines that appear after this entry are the installation components that have been rolled back because the installation was unsuccessful.

More information

[Choosing a method to install the client using the Client Deployment Wizard](#)

Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client

If you have trouble with client and server communication, you should first check to make sure that there are no network problems. You should also check network connectivity before you call Symantec Technical Support.

You can check the communication between the client and the management server in several ways.

Table 205: Checking the connection between the management server and the client

What to check	Solution
Look on the client to see if the client connects to the management server	You can download and view the troubleshooting file on the client to verify the communication settings. See: • Symantec Endpoint Protection client status icons • Checking the connection to the management server on the client computer • Investigating protection problems using the troubleshooting file on the client
Test the connectivity between the client and the management server	You can perform several tasks to check the connectivity between the client and the management server. • See: Enabling and viewing the Access log to check whether the client connects to the management server • Ping the management server from the client computer. See: Using the ping command to test the connectivity to the management server • Use a Web browser on the client computer to connect to the management server. See: Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client
Check that the management server uses the correct server certificate	If you reinstalled Symantec Endpoint Protection Manager, check that the correct server certificate was applied. If the management server uses a different server certificate, the server still downloads content, but the client cannot read the content. If the management server uses the wrong server certificate, you must update it. See: • Updating or restoring a server certificate You can verify that the management server uses the wrong server certificate by checking the following items: • The client does not display the green dot in the taskbar, which indicates that it does not communicate with the management server. See: Checking whether the client is connected to the management server and is protected • The client does not receive policy updates from the management server. • The management server shows that it does connect with the client. See: Symantec Endpoint Protection client status icons
Check for any network problems	You should verify that there are no network problems by checking the following items: • Test the connectivity between the client and the management server first. If the client computer cannot ping or Telnet to the management server, you should verify the DNS service for the client. • Check the client's routing path. • Check that the management server does not have a network problem. • Check that the Symantec Endpoint Protection firewall (or any third-party firewall) does not cause any network problems.
Check the debug logs on the client	You can use the debug log on the client to determine if the client has communication problems. See: • Checking the debug log on the client computer • Checking the inbox logs on the management server
Recover lost client communication	If the clients have lost the communication with a management server, you can use a tool to recover the communication file. See: Restoring client-server communication settings with the SylinkDrop tool

If Symantec Endpoint Protection Manager displays logging errors or HTTP error codes, see the following article:

[Symantec Endpoint Protection Manager Communication Troubleshooting](#)

Checking the connection to the management server on the client computer

If you have a managed client, you can check your connection to the management server. If you are not connected to the management server, you can request that your client connect. See:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

To check the connection to the management server on the client computer

1. On the **Status** page, click **Help > Troubleshooting**.
2. In the **Troubleshooting** dialog box, click **Connection Status**.
3. In the **Connection Status** pane, you can see the last attempted connection and the last successful connection.
4. To reestablish a connection with the management server, click **Connect Now**.

Investigating protection problems using the troubleshooting file on the client

To investigate client problems, you can examine the `Troubleshooting.txt` file on the client computer. The `Troubleshooting.txt` file contains information about policies, virus definitions, and other client-related data.

Symantec Technical Support might request that you email the `Troubleshooting.txt` file. See:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

To export the troubleshooting file from the client

1. On the client computer, open the client.
2. In the client, click **Help > Troubleshooting**.
3. In the **Management** pane, under **Troubleshooting Data**, click **Export**.
4. In the **Save As** dialog box, accept the default troubleshooting file name or type a new file name, and then click **Save**.

You can save the file on the desktop or in a folder of your choice.

5. Using a text editor, open `Troubleshooting.txt` to examine the contents.

Enabling and viewing the Access log to check whether the client connects to the management server

You can view the Apache HTTP server Access log on the management server to check whether the client connects to the management server. If the client connects, the client's connection problem is probably not a network issue. Network issues include the firewall blocking access, or networks not connecting to each other.

You must first enable the Apache HTTP server Access log before you can view the log.

NOTE

Disable the log after you view it because the log uses unnecessary CPU resources and hard disk space.

For more information, see:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

NOTE

The default for `SEPM_Install` is `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager`.

To enable the Apache HTTP server Access log

1. In a text editor, open the file `SEPM_Install\apache\conf\httpd.conf`.
2. In the `httpd.conf` file, remove the hash mark (#) from the following text string and then save the file:

```
#CustomLog "logs/access.log" combined
```

-
3. Stop and restart the Symantec Endpoint Protection Manager service and Apache HTTP server.

[Stopping and starting the management server service](#)

[Stopping and starting the Apache Web server](#)

To view the Apache HTTP server Access log

1. On the management server, open the file `SEPM_Install\apache\logs\access.log`.
2. Look for a client computer's IP address or host name, which indicates that clients connect to the Apache HTTP server.
3. Disable the Apache HTTP server Access log.

Stopping and starting the Apache Web server

When you install Symantec Endpoint Protection Manager, it installs the Apache Web server. The Apache Web server runs as an automatic service. You may need to stop and restart the Web server to enable the Apache HTTP Server Access log. See:

[Enabling and viewing the Access log to check whether the client connects to the management server](#)

To stop the Apache Web server	From a command prompt, type: <code>net stop semwebsrv</code>
To start the Apache Web server	From a command prompt, type: <code>net start semwebsrv</code>

Using the ping command to test the connectivity to the management server

You can try to ping the management server from the client computer to test connectivity. See:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

To use the ping command to test the connectivity to the management server

1. On the client, open a command prompt.
2. Type the ping command. For example:

```
ping name
```

where name is the computer name of the management server. You can use the server IP address in place of the computer name. In either case, the command should return the server's correct IP address.

If the ping command does not return the correct address, verify the DNS service for the client and check its routing path.

Using a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client

You can use a web browser on the client computer to test the connectivity between the management server and the client. This method helps determine whether the problem is with the connection or network, or with the client itself.

You can also check the connection between the management server and the client computer by using the following methods:

- Checking whether the Symantec Endpoint Protection client status icon shows a green dot. See:
[Symantec Endpoint Protection client status icons](#)
- Checking the connection status on the Symantec Endpoint Protection client. See:
[Checking the connection to the management server on the client computer](#)

To use a browser to test the connectivity to Symantec Endpoint Protection Manager on the Symantec Endpoint Protection client

1. On the client computer, open a web browser, such as Internet Explorer.

2. In the browser command line, type the following command:

```
http://SEPMServer:8014/secars/secars.dll?hello,secars
```

where SEPMServer is the management server's DNS name, NetBIOS name, or IP address.

IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets: `http://[SEPMServer]:port number`

3. When the webpage appears, look for one of the following results:

- If the word **OK** appears, the client computer connects to the management server. Check the client for a problem.
- If the word **OK** does not appear, the client computer does not connect to the management server. Check the client's network connections and that network services are running on the client computer. Verify the DNS service for the client and check its routing path. See:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

Checking the debug log on the client computer

You can check the debug log on the client. If the client has communication problems with the management server, status messages about the connection problem appear in the log. See:

[Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)

You can check the debug log by using the following methods:

- In the client, on the Help and Support menu, in the Troubleshooting dialog box, you can click **Edit Debug Log Settings** and type a name for the log. You can then click **View Log**.
- You can use the Windows registry to turn on debugging in the client.
You can find the Windows registry key in the following location:
`HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on`

Checking the inbox logs on the management server

You can use a Windows registry key to generate logs about activity in the management server inbox. When you modify the Windows registry key, the management server generates the logs (ersecreg.log and exsecars.log). You can view these logs to troubleshoot client and server communication. See:

- [Troubleshooting connectivity problems between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection client](#)
- [Checking the debug log on the client computer](#)

To check the inbox logs on the management server

1. On the management server, under `HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM`, set the `DebugLevel` value to 3.

The inbox appears in the following default location on the management server computer: `SEPM_Install\data\inbox\log`

The default for `SEPM_Install` is `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager`.

2. Open the log with Notepad.

Troubleshooting the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux

Use these tips to troubleshoot issues with the Symantec Endpoint Protection Linux Agent or the Symantec Single Agent for Linux.

NOTE

Both the Symantec Single Agent for Linux and the Symantec Endpoint Protection Linux Agent are referred to in this topic as the Linux Agent.

The table below shows the resources for troubleshooting the Linux Agent (as of 14.3 RU1).

Table 206: Resources for troubleshooting the Symantec Linux Agent

Action	Description
Checking the status of the agent.	To check the version and connection status of the agent and to confirm that the modules are loaded and daemons are running, navigate to <code>/usr/lib/symantec</code> and run the following command: <code>./status.sh</code>
Checking the versions of the agent packages.	Navigate to <code>/usr/lib/symantec</code> and run the following command: <code>./version.sh</code>
Viewing the logs.	You find the Symantec Linux Agent logs at the following locations: • AMD log - provides information related to scanning. <code>/var/log/sdcssllog/amd.log</code> • CAF log - provides information related to agent activities such as communication with the server, enrollment, commands, events, policy version, content version, etc. <code>/var/log/sdcssl-cafflog/cafagent.log</code> • Agent log - provides some consolidated information related to agent activities (scan info, update info). <code>/var/log/sdcssllog/SISIDSEvents*.csv</code> • CVE log - provides information related to communication between Symantec Endpoint Protection Manager and the agent. <code>/var/log/sdcssl-cafflog/cve.log</code>
Collecting the logs into a zip file.	You can use <code>GetAgentInfo</code> script to collect all log files into a ZIP file that you can send to customer support. 1. Login to Symantec Linux Agent system. 2. Navigate to <code>/opt/Symantec/sdcsslagent/IPS/tools/</code>. 3. Run <code>./getagentinfo.sh</code> as root. 4. A ZIP file will be created in <code>/tmp/</code> directory. The name of the file will look similar to <code>20201208_184935_0001_CU_mihsan-rhel8.zip</code> <code>-out <directory></code> lets you change the location and the name of the generated ZIP file.

Troubleshooting communication problems between Symantec Endpoint Protection Manager and the console or the default database

If you have a connection problem with the Symantec Endpoint Protection Manager console or the default database, you may see one of the following symptoms:

- The management server service (semsrv) stops.
- The management server service does not stay in a started state.
- The Home, Monitors, and Reports pages display an HTTP error.
- The Home, Monitors, and Reports pages are blank.
- The Home, Monitors, and Reports pages display a continuously loading progress bar, without displaying any content.

All of these issues display a Java -1 error in the Windows Event log. To find the specific cause for the Java -1 error, look in the scm-server log. The scm-server log is located by default in the following location:

SEPM_Install\tomcat\logs\scm-server-0.log

The default for SEPM_Install is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager.

Table 207: Checking the communication with the console or database

What to check	Description
Test the connectivity between the database and the management server.	You can verify that the management server and the database communicate properly. See: Verifying the connection with the database
Check that the management server heap size is correct.	If you cannot log on to the management server's remote console, you may need to increase the Java heap size. You may also see an out-of-memory message in the scm-server log. For more information on the default heap sizes, see: Determining the default settings for the network sizes that you select during installation of the Symantec Endpoint Protection Manager
Check that the management server is not running multiple versions of PHP.	You can check whether the management server runs multiple software packages that use different versions of PHP. PHP checks for a global configuration file (php.ini). If there are multiple configuration files, you must force each product to use its own interpreter. When each product uses the correct version of PHP associated with it, the management server operates properly.
Check the system requirements.	You can check whether both the client and the management server run the minimum or the recommended system requirements. For the most current system requirements, see: Release notes, new fixes, and system requirements for all versions of Endpoint Protection

Verifying the management server connection with the database

The management server and the database may not communicate properly. You should verify that the database runs and then test the connection between the server and the database.

Table 208: Verifying the database connection

Database type	Perform these steps
Microsoft SQL Server Express database (as of 14.3 RU1)	• Verify that the SQL Server Express service runs and that the sqlserver.exe process listens to TCP port 2638. • Test the ODBC connection.
Embedded Sybase database (14.3 MP1 and earlier)	• Verify that the Symantec Embedded Database service runs and that the dbsrv9.exe process listens to TCP port 2638. • Test the ODBC connection.

6. Click **Login**.
7. On the **Login** tab, in the **User ID** text box, type `dba`.
8. In the **Password** text box, type the password for the database.
This password is the one that you entered for the database when you installed the management server.
9. Click **Database**.
10. On the **Database** tab, in the **Server name** text box, type:
`\\servername\instancename`
If you use the English version of Symantec Endpoint Protection Manager, type the default, `sem5`. Otherwise, leave the Server name text box blank.
11. On the **ODBC** tab, click **Test Connection** and verify that it succeeds.
12. Click **OK**.
13. Click **OK**.

To verify communication to the Microsoft SQL Server database:

1. On the management server computer, click **Start > Control Panel > Administrative Tools**.
2. In the **Administrative Tools** dialog box, double-click **Data Sources (ODBC)**.
3. In the **ODBC Data Source Administrator** dialog box, click **System DSN**.
4. On the **System DSN** tab, double-click **SymantecEndpointSecurityDSN**.
5. In the **Server** drop-down list, verify that the correct server and instance is selected.
6. Click **Next**.
7. For Login ID, type `sa`.
8. In the **Password** text box, type the password for the database.
This password is the one that you entered for the database when you installed the management server.
9. Click **Next** and make sure that `sem5` is selected for the default database.
10. Click **Next**.
11. Click **Finish**.
12. Click **Test Data Source** and look for the result that states:

TESTS COMPLETED SUCCESSFULLY!

Client and server communication files

The communication settings between the client and server and other client settings are stored in files on the client computer.

Table 209: Client files

File name	Description
SerDef.dat	An encrypted file that stores communication settings by location. Each time the user changes locations, the SerDef.dat file is read and the appropriate communication settings for the new location are applied to the client.
sylink.xml	Stores the global communication settings. This file is for internal use only and should not be edited. It contains settings from the Symantec Endpoint Protection Manager. If you edit this file, most settings will be overwritten by the settings from the management server the next time the client connects to the management server.
SerState.dat	An encrypted file that stores information about the user interface, such as the client's screen size, whether the client's console for Network and Host Exploit Mitigation appears, and whether Windows services appear. When the client starts, it reads this file and returns to the same user interface state as before it was stopped.

Troubleshooting reporting issues

You should be aware of the following information when you use reports:

- Timestamps, including client scan times, in reports and logs are given in the user's local time. The reporting database contains events in Greenwich Mean Time (GMT). When you create a report, the GMT values are converted to the local time of the computer on which you view the reports.
- If managed clients are in a different time zone from the management server, and you use the **Set specific dates** filter option, you may see unexpected results. The accuracy of the data and the time on both the client and the management server may be affected.
- If you change the time zone on the server, log off of the console and log on again to see accurate times in logs and reports.
- In some cases, the report data does not have a one-to-one correspondence with what appears in your security products. This lack of correspondence occurs because the reporting software aggregates security events.
- You can use SSL with the reporting functions for increased security. SSL provides confidentiality, the integrity of your data, and authentication between the client and the server. See the article:
[Enabling SSL communications between a Symantec Endpoint Protection Manager and its clients](#)
- Risk category information in the reports is obtained from the Symantec Security Response Web site. Until the Symantec Endpoint Protection Manager console is able to retrieve this information, any reports that you generate show Unknown in the risk category fields.
- The reports that you generate give an accurate picture of compromised computers in your network. Reports are based on log data, not the Windows registry data.
- If you get database errors when you run a report that includes a large amount of data, you might want to change database timeout parameters. See:
[Changing timeout parameters for reviewing reports and logs](#)
- If you get CGI or terminated process errors, you might want to change other timeout parameters. For more information, see the following article:
[SEPM Reporting does not respond or shows a timeout error message when querying large amounts of data.](#)
- If you have disabled the use of loopback addresses on the computer, the reporting pages do not display. See:
[Accessing reporting pages when the use of loopback addresses is disabled](#)

Changing timeout parameters for reviewing reports and logs

If database errors occur when you view either reports or logs that contain a lot of data, you can make the following changes:

- Change the database connection timeout
- Change the database command timeout

The reporting defaults for these values are as follows:

- Connection timeout is 300 seconds (5 minutes)
- Command timeout is 300 seconds (5 minutes)

To change database timeout values in Reporter.php and Reporter2.php

1. Browse to the following default folder on the Symantec Endpoint Protection Manager server:
`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php\Include\Resources`
2. Open the Reporter.php and Reporter2.php files with a plain-text editor, such as Notepad.
3. Find the **\$CommandTimeout** and **\$ConnectionTimeout** lines and increase the value (in seconds). If either line does not exist, create it. For example, to increase the timeout period to 10 minutes, change the line to the following value:
`$CommandTimeout = 600;`
`$ConnectionTimeout = 600;`
Add these new lines before the following characters: `?>`
4. Save and close the Reporter.php and Reporter2.php files.

NOTE

If you specify zero, or leave the fields blank, the default setting is used.

If you get CGI or terminated process errors, you might want to change the following parameters:

- `max_execution_time` parameter in the `Php.ini` file
- The Apache timeout parameters, `FcgidIOTimeout`, `FcgidBusyTimeout`, and `FcgidIdleTimeout`, in the `httpd.conf` file

To change the `max_execution_time` parameter in `Php.ini`

1. Browse to following default folder on the Symantec Endpoint Protection Manager server:
`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Php`
2. Right-click the `Php.ini` file, and then click **Properties**.
3. On the **General** tab, uncheck **Read-only**.
4. Click **OK**.
5. Open the `Php.ini` file with a plain-text editor, such as Notepad.
6. Locate the `max_execution_time` entry and increase the value (in seconds). For example, to increase the timeout to 10 minutes, change the line to the following value:
`max_execution_time=600`
7. Save and close the `Php.ini` file.
8. Right-click the `Php.ini` file, and then click **Properties**.
9. On the **General** tab, check **Read-only**.
10. Click **OK**.

To change Apache timeout parameters in `httpd.conf`

1. Browse to the following default folder on the Symantec Endpoint Protection Manager server:
`C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\apache\conf`
2. Open the `httpd.conf` file with a plain-text editor, such as Notepad.
3. Locate the following lines and increase the values (in seconds):
 - `FcgidIOTimeout 1800`
 - `FcgidBusyTimeout 1800`
 - `FcgidIdleTimeout 1800`
4. Save and close the `httpd.conf` file.

Accessing reporting pages when the use of loopback addresses is disabled

If you have disabled the use of loopback addresses on the computer, the reporting pages do not display. If you try to log on to the Symantec Endpoint Protection Manager console or to access the reporting functions, you see the following error message:

Unable to communicate with Reporting component

The **Home**, **Monitors**, and **Reports** pages are blank; the **Policies**, **Clients**, and **Admin** pages look and function normally.

To get the **Reports** components to display when you have disabled loopback addresses, you must associate the word `localhost` with your computer's IP address. You can edit the Windows hosts file to associate `localhost` with an IP address. See:

[Logging on to reporting from a standalone web browser](#)

To associate localhost with the IP address on computers running Windows

-
1. Change directory to the location of your hosts file.

By default, the hosts file is located in %SystemRoot%\system32\drivers\etc

2. Open the hosts file with an editor.

3. Add the following line to the hosts file:

```
IPAddress localhost #to log on to reporting functions
```

where you replace IPAddress with your computer's IP address. You can add any comment you want after the pound sign (#). For example, you can type the following line:

```
192.168.1.100 localhost # This entry is the IPv4 for my console computer
```

```
2001:db8:85a3::8a2e:370:7334 localhost # This entry is the IPv6 address for my console computer
```

IPv6 is supported as of version 14.2.

4. Save and close the file.

What you should know before you run Symantec Power Eraser from the Symantec Endpoint Protection Manager console

Symantec Power Eraser is a free virus removal tool to remove malware and threats from your computer. Power Eraser is provided with the product and does not need to be installed.

Typically, you need to run a Power Eraser analysis when the Risk log shows a failed repair and recommends that you run Power Eraser. You also might run Power Eraser when a computer becomes unstable and appears to have malware or a virus that cannot be removed.

Symantec Power Eraser provides aggressive scanning and analysis to help resolve issues with heavily infected Windows computers. Because Power Eraser analysis is aggressive, it sometimes flags the critical files that you might need. Power Eraser can produce more false positives than virus and spyware scans.

WARNING

You should run Power Eraser only in emergency situations, such as when computers exhibit instability or have a persistent problem. Typically, you run Power Eraser on a single computer or small group of computers. You should not run other applications at the same time. In some cases, a regular scan event alerts you to run a Power Eraser analysis.

For Norton Power Eraser, see: [Download and run Norton Power Eraser - Free virus and malware removal tool for Windows](#)

Differences between using Power Eraser from Symantec Endpoint Protection Manager or locally with the SymDiag tool

You can run Power Eraser remotely from the management console on your Windows clients. Symantec Endpoint Protection does not include an option to launch Power Eraser directly from the client. However, a user on the client computer can download the SymDiag tool and run Power Eraser from the tool.

- If you use the SymDiag tool, Power Eraser detections do not appear in the Symantec Endpoint Protection Manager logs.
- When you run Power Eraser from the console, Power Eraser does not examine the user-specific load points, registrations, and folders that the SymDiag tool examines.

NOTE

Make sure that you do not run Power Eraser from the console and locally with the SymDiag tool at the same time. Otherwise, you might negatively affect the computer performance.

Power Eraser consumes a large amount of computer resources. Power Eraser files can also consume a large amount of space on the computer if you run Power Eraser on a computer multiple times. During each analysis, Power Eraser saves detection information in the files that it stores in the Symantec Endpoint Protection application folder. The files are purged when the client purges the logs.

Differences between Power Eraser scans and virus and spyware scans

Power Eraser is different from regular scans in the following ways:

14.3 RU5 and later	14.3 RU4 and earlier
Power Eraser scans and virus and spyware scans both run an active scan and a full scan. However, Power Eraser uses the more aggressive High Intensity Detection (HID) scans that employ advanced machine learning (AML) techniques. The AML engine determines if a file is good or bad through a learning process. The AML engine recognizes malicious attributes and defines the rules that the AML engine uses to make detections.	Unlike a full virus and spyware scan, Power Eraser does not scan every file on the computer. Power Eraser examines load points and load point disk locations as well as running processes and installed services.
Power Eraser automatically remediates detections based on the scan threshold level. HID scans use a threshold level (from 1 to 5) that triggers a detection action, either blocking (level 1 and 2) or logging (level 3 and 4). - Blocked detections are convicted files that are either cleaned first, and if unsuccessful, then quarantined (viruses) or quarantined first (security risks). - Logged detections are suspicious files that are sent to the Scan log or the Risk log. You must review the detection list in either log and select an action from the log.	Power Eraser does not automatically remediate detections. Power Eraser detections are not automatically sent to the Quarantine. You must review the detection list in the Scan log or Risk log and must select an action from the log. You can choose to remove the detection or mark the detection as safe (leave alone). You can also restore (undo) a removed detection.
Power Eraser takes precedence over virus and spyware scans. When you run Power Eraser, Symantec Endpoint Protection cancels any virus and spyware scan in progress. If you manage Symantec Endpoint Protection in hybrid mode, Power Eraser blocks detections at either level 2 or the level of the Intensive Protection policy, whichever value is higher. For example, if the cloud console Intensive Protection policy block level is set to 3, Power Eraser blocks at 3.	Power Eraser takes precedence over virus and spyware scans. When you run Power Eraser, Symantec Endpoint Protection cancels any virus and spyware scan in progress.
Only 14.3 RU4 or earlier client computers in rootkit mode are restarted.	Power Eraser can run in regular mode or in rootkit mode. The rootkit mode requires a restart before the scan launches. Also, if you choose to remove any Power Eraser detection, the computer must be restarted for the remediation to complete.
Power Eraser runs on Windows clients only, while virus and spyware scans run on Windows, Mac, and Linux clients	Same as for 14.3 RU5 and later.

Overview of the high-level steps that you perform when you must run Power Eraser

You perform two high-level steps when you run Power Eraser from the console:

- Start a Power Eraser analysis on one computer or a small group of computers. Power Eraser may or may not remediate detections automatically, based on the client version.
- Use the Risk log or Scan log to review Power Eraser detections and manually request that Power Eraser remove any detections that you determine are threats. You can also acknowledge the detections that you want to ignore and leave alone.

Learn how to run Power Eraser from the console and how to make sure that you configure the console settings correctly. See:

[Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)

Overview of the Symantec Endpoint Protection Manager policy settings that affect Power Eraser

The following policy settings affect Power Eraser:

- Scan settings for user interaction
When you let users cancel any virus and spyware scan, you also let them cancel any Power Eraser analysis. However, users cannot pause or snooze Power Eraser. See:
[Allowing users to view scan progress and interact with scans on Windows computers](#)
- Exceptions policy
Power Eraser honors the following virus and spyware exceptions: file, folder, known risk, application, and trusted web domain. Power Eraser does not honor extension exceptions. See:
[Creating exceptions for Virus and Spyware scans](#)
- Log retention settings
You can take action on Power Eraser detections as long as the detections appear in the logs. The logs are purged after the time period that is specified in the Virus and Spyware Protection policy. By default, log events are available for 14 days. You can modify the log retention setting, or after the events expire, you can run another scan and re-populate the logs. See:
[Modifying log handling and notification settings on Windows computers](#)
- Restart options (14.3 RU4 or earlier computers)
You can configure the restart settings specifically for rootkit analysis when you choose to run Power Eraser in rootkit detection mode. The administrator must have restart privileges. After you choose to remove a Power Eraser detection, the computer uses the group restart settings. Power Eraser does not use the rootkit restart settings to restart and complete a remediation. See:
[Restarting the client computers from Symantec Endpoint Protection Manager](#)
- Reputation queries
Power Eraser uses the Symantec Insight server in the cloud when it scans and makes decisions about files. If you disable reputation queries, or if the client computer cannot connect to the Insight server, Power Eraser cannot use Symantec Insight. Without Symantec Insight, Power Eraser makes fewer detections, and the detections it makes are more likely to be false positives. Reputation queries are enabled when the **Allow Insight lookups for threat detection** option is enabled. The option is enabled by default. See:
[How Symantec Endpoint Protection uses Symantec Insight to make decisions about files](#)
- Submissions
Symantec Endpoint Protection sends the information about Power Eraser detections to Symantec when the **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence** option is enabled. The option is enabled by default. See:
[Understanding server data collection and client submissions and their importance to the security of your network](#)

More information

[Troubleshooting computer issues with the Symantec Diagnostic Tool \(SymDiag\)](#)

Tasks to perform when you must run Power Eraser from the Symantec Endpoint Protection Manager console

WARNING

Use Power Eraser carefully. The analysis is aggressive and prone to false positives.

For more information, see:

[What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console](#)

You can run Power Eraser from Symantec Endpoint Protection Manager on Windows client computers only.

Table 210: Tasks to perform when you must run Power Eraser from the Symantec Endpoint Protection Manager console

Task	Description
Make sure that your clients have Internet connectivity	Your client computers require Internet access so that Power Eraser can use Symantec Insight reputation data to make decisions about potential threats. Intermittent or non-existent Internet access means that Power Eraser cannot use Symantec Insight. Without Symantec Insight, Power Eraser makes fewer detections, and the detections it produces are more likely to be false positives.
Set limited administrator privileges to run Power Eraser	To run Power Eraser on client computers, limited administrators must have the following command access rights: • Power Eraser Analysis • Restart Client Computers (14.3 RU4 and earlier clients that run Power Eraser with rootkit detection) For more information, see: Adding an administrator account and setting access rights
Set the log retention policy	The log retention setting affects how long the events are available for you to perform the Power Eraser remediate and restore actions. You can modify the log retention setting if you want more time to consider these actions. Alternately, you can run Power Eraser again to re-populate the logs. The log retention setting is part of the miscellaneous options in the Virus and Spyware Protection policy. See: Modifying log handling and notification settings on Windows computers
Run the Power Eraser analysis from Symantec Endpoint Protection Manager	You can issue the Power Eraser command from several places in Symantec Endpoint Protection Manager: • Clients page • Computer Status log • Risk log Note: A user on the client computer cannot run Power Eraser directly from the client user interface. Power Eraser is available as part of the SymDiag tool. However, if a client user runs the tool, the resulting logs that include Power Eraser detections are not sent to Symantec Endpoint Protection Manager. For more information, see: Starting Power Eraser analysis from Symantec Endpoint Protection Manager You can view the status of the command in the Computer Status log. You can filter the log so that only Power Eraser commands appear for ease of viewing.
Cancel a Power Eraser command or action on a client computer	To cancel the Power Eraser command, use the Command Status log. Note: You cannot cancel Power Eraser if the restart prompt appears on the client computer. After the restart, only the computer user can cancel Power Eraser if the Virus and Spyware Protection policy lets users cancel scans. If you cancel the Power Eraser command, you also cancel any pending actions that are associated with any Power Eraser analysis, including any remediation or undo actions. For more information, see: Running commands on client computers from the console

Task	Description
View Power Eraser detections from the logs	You can view Power Eraser detections from the following logs in Symantec Endpoint Protection Manager: • Scan log The Scan log has a Scan type filter to display only Power Eraser results. The view also indicates whether or not scan results are pending. You can select Detections in the filtered view to display the Power Eraser Detections view. • Risk log The Risk log provides a similar filter for Power Eraser detections. However, the Risk log does not show whether or not scan results are pending. • Computer Status log The Computer Status log might include report icons in the Infected column. The event details icon links to a report that shows all current threats that cannot be remediated. The report includes log-only detections and unresolved detections. The report might recommend that you run Power Eraser on some computers. A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action. These icons also appear in the Health State column on the Clients page. For more information, see: Viewing logs
Check for the notifications that recommend that you run Power Eraser on client computers	By default, the administrator receives a notification when a regular scan cannot repair an infection and Power Eraser is recommended. You can check for the Power Eraser recommended notification on the Monitors > Notifications > Notification Conditions page. See: Viewing and acknowledging notifications
View Power Eraser detections on the Command Status page	You can access reports about Power Eraser detections on the Command Status page. An event details icon appears in the Completion Status column. The icon links to a report that shows information about detections that were made by the Start Power Eraser Analysis command and any other scan command. The command status details option gives you information about a particular scan. You can click the event details icon to get information about a particular client computer. See: Running commands on client computers from the console
View Power Eraser detections from the Clients tab	You can access reports about Power Eraser detections from the Clients tab on the Clients page. Report icons appear in the Health State column if information is available. The event details icon links to a report that shows all current threats that cannot be remediated. The report includes any Power Eraser detections. A Power Eraser icon links to a report that shows any Power Eraser detections on the computer that require administrator action. The icons also appear in the Computer Status log. For more information, see: Viewing the protection status of client computers
Remediate or restore Power Eraser detections from the Scan log or Risk log in Symantec Endpoint Protection Manager	In 14.3 RU5 and later, Power Eraser quarantines detected threats if the threat level is below a certain threshold. Power Eraser does not automatically remediate detected threats in the following cases: • For 14.3 RU4 and earlier clients. • For 14.3 RU5 detections that are logged as suspicious and are above a certain threshold. Power Eraser analysis is aggressive and might detect many false positives. After you determine whether the detection requires remediation, you must initiate a remediation manually. You can also undo (restore) a Power Eraser detection that was quarantined. For more information, see: Responding to Power Eraser detections

Starting Power Eraser analysis from Symantec Endpoint Protection Manager

You can run Power Eraser to analyze and detect persistent threats on a single computer or a small group of computers. See:

[What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console](#)

After Power Eraser detects potential risks, you view the risks and determine which risks are threats. In 14.3 RU4 and earlier, Power Eraser does not automatically remediate risks. You must manually run Power Eraser to remediate the risks that you determine are threats. You can also run Power Eraser on a particular threat or threats that other protection features detect. Power Eraser runs on the computers that are associated with the detection. See:

- [Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)
- [Responding to Power Eraser detections](#)

NOTE

When you run Power Eraser and the restart option message appears on a 14.3 RU4 and earlier client computer, the administrator or the user cannot cancel Power Eraser. After the restart, the user can cancel Power Eraser if the Virus and Spyware Protection policy lets users cancel scans.

To start Power Eraser analysis from the Clients page

1. On the **Clients** page, on the **Clients** tab, select the computers that you want to analyze.
If you select many computers, you might adversely affect the performance of your network.
2. Under **Tasks**, click **Run command on computers**, and then click **Start Power Eraser Analysis**.
3. In the **Choose Power Eraser Type** dialog, select which mode you want to run the scan in.
 - 14.3 RU5 and later: For the full disk option, you do not need to restart the computers unless 14.3 RU4 and earlier clients are in the group.
 - 14.3 RU4 and earlier: For rootkit mode, you can set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.
4. Click **OK**.
Power Eraser runs on the selected computers. You can cancel the command on the **Command Status** tab on the **Monitors** page.

To start Power Eraser analysis from the Computer Status log

1. In the console, in the sidebar, click **Monitors** and select the **Logs** tab.
2. In the **Log type** list box, select the **Computer Status** log, and then click **View Log**.
3. Select the computers on which you want to run Power Eraser and select **Start Power Eraser Analysis** from the **Commands** drop-down box.
If you select many computers, you might adversely affect the performance of your network.
4. Click **Start**.
5. In the **Choose Power Eraser Type** dialog, select a scan type.
6. Click **OK**.
Power Eraser runs on the selected computers. You can cancel the command on the **Command Status** tab.

To start Power Eraser analysis from the Risk log

1. In the console, in the sidebar, click **Monitors** and select the **Logs** tab.
2. In the **Log type** list box, select the **Risk** log, and then click **View Log**.
3. Select the risks on which you want to run Power Eraser. In the **Event Action** column, you might see an alert to run Power Eraser.

- You can run Power Eraser on any risk in the log.
- From the **Action** drop-down or the **Action** column, select **Start Power Eraser Analysis**.
 - Click **Start**.
 - In the **Choose Power Eraser Type** dialog, select whether you want Power Eraser to run one of the following options:
 - 14.3 RU5 and later: Select either common infection locations or the full disk.
 - 14.3 RU4 and earlier: Select either without rootkit detection or with rootkit detection. For rootkit detections, you set the restart options. You must have administrator privileges to set restart options and run a rootkit scan.
 - Click **OK**.
- Power Eraser runs on the computers that are infected with the selected risks. You can cancel the command on the **Command Status** tab.

Responding to Power Eraser detections

Power Eraser remediates detections in different ways, depending on the client version.

Table 211: Power Eraser remediation

14.3 RU5 and later	14.3 RU4 and earlier
Power Eraser uses the High Intensity Detection (HID) scan engine, which detects threats as a confirmed risk or a confirmed suspicious risk. The HID scan handles these risks immediately. - Viruses are cleaned and if that fails, they are quarantined. - Security risks are quarantined, and if that fails, they are logged as suspicious files. You can manually remediate any suspicious file by quarantining it. If you think the file is a false positive, you create an exception using the Ignore suspicious file action.	Power Eraser does not remediate any detections to minimize false positives. Instead, you must request remediation for detected events from the logs after you review the detections and decide whether to remediate them or leave them alone. If you choose remediation, Power Eraser removes the files that are associated with the detection. However, you can restore the removed files until the logs are purged.

The log retention policy determines how long Power Eraser events are available. By default, the events are available for 14 days.

For more information, see:

- [Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)
- [What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console](#)

To respond to Power Eraser detections

- Make sure that the Power Eraser analysis completed.
 - The Computer Status log includes an icon that indicates the scan is complete.
 - The Scan log shows whether or not Power Eraser finished the analysis.
- In the Risk log or on the **Scan log > View detections** page, select a single detection or multiple detections to which to apply an action.
 - Next to a particular risk that is labeled **Potential risk found (Pending admin action)**, click the plus icon in the **Action** column.
 - Select multiple risks that are labeled **Potential risk found (Pending admin action)**, and then select the action from the **Action** drop-down menu.

3. Choose one of the following actions:

14.3 RU5 and later: Remediate suspicious file 14.3 RU4 and earlier: Delete risk that Power Eraser detected	Remediates the risk by removing it from the computer. Power Eraser saves a safe backup file that can be restored.
14.3 RU5 and later: Ignore suspicious file 14.3 RU4 and earlier: Ignore risk that Power Eraser detected	Acknowledges that you reviewed the detection and do not want to remediate the risk. Note: This action changes the event action to "Left alone by Admin" in the management console logs only. The acknowledgment does not update the corresponding event action on the client. The client log view continues to show the event action as "Pending analysis."

4. If you selected an action from the **Action** drop-down menu, click **Apply**.

If you selected **Ignore risk that Power Eraser detected**, the detection now appears as **Potential risk found (left alone)**.

You can restore a removed detection that is labeled **Potential risk found (Removed)** by selecting one of the following actions:

- 14.3 RU5 and later: **Restore from Quarantine**
- 14.3 RU4 and earlier: **Restore risk that Power Eraser deleted**

Table 212: Summary of Power Eraser detection states

Detection state	Description
Pending admin action	Power Eraser detected the risk as a potential threat. You should review the risk and decide if Power Eraser should remediate the risk or acknowledge the risk and leave it alone.
Restored	An administrator restored any files that were moved when an administrator requested that Power Eraser remediate the risk.
Quarantined (14.3 RU5)	Either Power Eraser or an administrator quarantined a confirmed risk or a confirmed suspicious risk.
Deleted (14.3 RU4 and earlier)	An administrator requested that Power Eraser remediate and delete the risk. When Power Eraser deletes a risk, it deletes the files that are associated with the risk but makes safe backup copies that can be restored. You might want to restore a deleted risk that you later determine is not a risk. You can restore the files until the log events are purged.
Left alone by admin	An administrator requested that Power Eraser leave the risk alone.

Appendices

Get reference information about client feature comparison, tools, command-line options, third-party installation tools.

This section includes a comparison of client features, tools included with Symantec Endpoint Protection, client command-line options, Windows installation with third-party tools, and more.

Symantec Endpoint Protection features based on platform

Refer to the following topics for more information:

- [Client protection features based on platform](#)
- [Management features based on platform](#)
- [AutoUpgrade differences based on platform](#)
- [Virus and Spyware Protection policy settings based on platform](#)
- [Intrusion Prevention and Memory Exploit Mitigation policy settings based on platform](#)
- [LiveUpdate policy settings based on platform](#)
- [Web and Cloud Access Protection policy settings based on platform](#)
- [Exceptions policy settings based on platform](#)
- [Device Control differences based on platform](#)

See also:

- [How to choose a client installation type](#)
- [Symantec Endpoint Protection feature dependencies for Windows clients](#)

Client protection features based on platform

Table 213: Client protection features based on platform

Client feature	Windows	Mac	Linux
Virus and Spyware Protection	Yes	Yes	Yes
Network and Host Exploit Mitigation • Network Threat Protection (intrusion prevention and firewall) • Memory Exploit Mitigation	Yes	• Firewall (as of 14.2) • Intrusion prevention Intrusion prevention for the Mac does not support custom signatures.	No
Proactive Threat Protection • Application and Device Control • Behavioral analysis (SONAR)	Yes	Device Control only	No
Host Integrity	Yes	No	No
Other protections • System lockdown • Tamper Protection	Yes	No	No

For more information, see:

- [About application control, system lockdown, and device control](#)
- [How Host Integrity works](#)

Management features based on platform

Table 214: Management features based on platform

Management feature	Windows	Mac	Linux
Deploy clients remotely from Symantec Endpoint Protection Manager • Web link and email • Remote push • Save package	Yes	Yes	Yes (Web link and email, Save package only)
Run commands on clients from the management server	• Scan • Update content • Update content and scan • Start Power Eraser analysis • Restart client computers • Enable Auto-Protect • Enable Network Threat Protection • Disable Network Threat Protection • Enable Download Insight • Disable Download Insight • Collect File Fingerprint List • Delete from Quarantine** • Cancel all scans**	• Scan • Update content • Update content and scan • Restart client computers (hard restart only) • Enable Auto-Protect • Enable/Disable Network Threat Protection	• Scan • Update content • Update content and scan • Enable Auto-Protect
Enable learned applications and Network Application Monitoring	Yes	No	No
Create locations and set security policies that apply by location	Yes	Yes	No You can view the client's location by the command line, but the client does not automatically switch locations based on specific criteria.
Set restart options for clients	Yes	No	No
Quick reports and Scheduled reports	• Audit • Application and Device Control • Compliance • Computer status • Deception • Network and Host Exploit Mitigation • Risk • Scan • System	• Computer status • Network and Host Exploit Mitigation • Risk • Scan	• Audit • Computer status • Risk • Scan • System

Management feature	Windows	Mac	Linux
Set size and retention options for logs that are maintained on the client computers	• System • Security and risk • Security • Traffic • Packet • Control	• System • Security and risk • Security	• System • Security and risk
Password protecting the client	Yes	Uninstall the client only	No
Move clients to a different management server by running the SylinkDrop tool	Yes	Yes	No
Move clients to a different management server by redeploying a client package with the Communication update package deployment option	Yes	Yes	No
Configure client submissions of pseudonymous security information to Symantec	Yes	Yes The Submissions setting only controls antivirus detection information. You can manually disable or enable intrusion prevention submissions on the clients. See: How to disable IPS data submission on Symantec Endpoint Protection for Mac clients	No
Configure clients to securely submit pseudonymous system and usage information	Yes	No	No
Manage the external communication between the management server and the clients	Yes	For LiveUpdate only	No
Manage client communication settings	• Management server lists • Communication mode (push or pull) • Set heartbeat interval • Upload learned applications • Upload critical events immediately • Set download randomization • Set reconnection preferences	• Management server lists • Communication mode (push or pull) • Set heartbeat interval • Set download randomization • Set reconnection preferences	• Management server lists • Communication mode (push or pull) • Set heartbeat interval

Management feature	Windows	Mac	Linux
Configure clients to use private servers - Endpoint Detection and Response server for Insight lookups and submissions - Private Insight server for Insight lookups	Yes	No	No
Automatically upgrade the Symantec Endpoint Protection client with AutoUpgrade	Yes	Yes	No
Automatically uninstall existing third-party security software	Yes	No	No
Automatically uninstall a problem Symantec Endpoint Protection client	Yes	No	No
Authentication for Symantec Endpoint Protection Manager log on	- Symantec Endpoint Protection Manager authentication - Two-factor authentication (14.2) - RSA SecurID authentication - Directory authentication - Smart card (PIV/CAC) authentication (14.2)	Not applicable	Not applicable

****You can only run these commands when viewing logs in Symantec Endpoint Protection Manager.**

For more information, see:

- [What are the commands that you can run on client computers?](#)
- [Tasks to perform when you need to run Power Eraser from the Symantec Endpoint Protection Manager console](#)
- [Managing the client-server connection](#)
- [Restoring client-server communications with Communication Update Package Deployment](#)

AutoUpgrade differences based on platform

Table 215: AutoUpgrade differences based on platform

Feature	Windows	Mac
Delta package	Standard and dark network clients receive a delta upgrade package that Symantec Endpoint Protection Manager generates. Embedded clients receive the full install package for an upgrade.	Mac clients always receive a full install package for upgrade.
Configuration options	Include a custom installation folder, and the option to uninstall existing security software.	Only for restart and upgrade. You cannot customize the installation folder. Installation logging always writes to /tmp/sepinstall.log.

Feature	Windows	Mac
Restart options after the upgrade completes in Client Install Settings	Include an option to not to restart the Windows client computer.	Do not include an option to not restart. Mac client computers always restart after the upgrade completes.
Upgrade Clients with Package wizard	You can modify the feature set on the Windows client.	You cannot modify the feature set on the Mac client.
Upgrades from an earlier version	You can upgrade to the latest version of Symantec Endpoint Protection from any earlier version, based on the supported upgrade path.	Yes, for 14.x and later.

For more information, see:

- [Upgrading client software with AutoUpgrade](#)
- [Supported upgrade paths to the latest version of Symantec Endpoint Protection 14.x](#)
- [How to choose a client installation type](#)

Virus and Spyware Protection policy settings based on platform

Table 216: Virus and Spyware Protection policy settings based on platform

Policy setting	Windows	Mac	Linux
Administrator-defined scans	• Scheduled scans (Active, Full, Custom) • On-demand scans • Triggered scans • Startup scans • Retry missed scheduled scans • Randomized scheduled scans	• Scheduled scans (Custom) • On-demand scans • Retry missed scheduled scans	• Scheduled scans (Custom) • On-demand scans • Retry missed scheduled scans (14.3 RU1)
Auto-Protect	• Enable Auto-Protect • Scan all files • Scan only selected extensions • Determine file types by examining file contents • Scan for security risks • Scan files on remote computers • Scan when files are accessed, modified, or backed up • Scan floppies for boot viruses, with the option to delete the boot virus or log it only • Always delete newly created infected files or security risks • Preserve file times • Tune scan performance for scan speed or application speed • Emulator for packed malware	• Enable Auto-Protect • Automatically repair infected files • Quarantine files that cannot be repaired • Scan compressed files • Scan all files • Scan only selected folders • Scan everywhere except in selected folders • Scan for security risks Scan on mount, current clients: • Data disks • All other disks and devices	• Enable Auto-Protect • Scan all files • Scan only selected extensions (removed in 14.3 RU1) • Scan removable media • Scan for security risks • Scan files on remote computers • Scan when files are accessed or modified • Scan inside compressed files

Policy setting	Windows	Mac	Linux
Email scans	- Microsoft Outlook Auto-Protect - Internet email Auto-Protect (removed in 14.2 RU1) - Lotus Notes Auto-Protect (removed in 14.2 RU1)	No	No
What to scan	- Additional locations - Memory - Selected folders - Selected extensions - Storage migration locations - Files inside compressed files - Security risks	- All or selected folders - Hard drives and removable drives - Files inside compressed files	- All files - All or selected folders - Selected extensions - Files inside compressed files - Security risks
User-defined scans (client)	- Active scan - Full scan - Custom scan of individual folders, files, and extensions	- Full scan - Custom scan of individual folders and files	- Full scan - Custom scan of individual folders and files
Define remediation actions for detections	- Clean (only applies to malware) - Quarantine - Delete - Leave alone (log only) The actions apply to categories of malware and security risks that Symantec periodically updates.	- Repair infected files - Quarantine files that cannot be repaired	(14.3 MP1 and earlier) - Clean (only applies to malware) - Quarantine - Delete - Leave alone (log only)
Set actions to take while a scan is running	- Stop the scan - Pause a scan - Snooze a scan - Scan only when the computer is idle	Yes - Stop a scan - Pause a scan - Snooze a scan before it begins - Scan only when the computer is idle	No
Download Insight	Yes	No	No
Insight lookups for threat detection	Yes	No	No
Bloodhound	Yes	No	Yes
Behavioral analysis (SONAR)	Yes	No Yes	No
Early Launch Anti-Malware Driver	Windows 8 and later, and Windows Server 2012 and later	No	No
Power Eraser	Yes	No	No
Endpoint Detection and Response enablement	Yes	No	No
Shared Insight Cache	Yes	No	No
Virtual Image Exception	Yes	No	No

For more information, see:

- [Preventing and handling virus and spyware attacks on client computers](#)
- [Using Symantec Endpoint Protection in virtual infrastructures](#)

Intrusion Prevention and Memory Exploit Mitigation policy settings based on platform

Table 217: Intrusion Prevention policy settings based on platform

Policy setting	Windows	Mac
Exceptions for intrusion prevention signatures	Yes Note: Custom exceptions are not supported for Browser Protection signatures.	Yes
Show or hide user notifications	Yes	Yes
Enable or disable excluded hosts	Yes	Yes
Custom IPS signatures	Yes	No
Enable or disable Network Intrusion Prevention	Yes	Yes
LiveUpdate updates IPS content	Yes	Yes
The management server updates IPS content	Yes	No **
Client package includes IPS	Yes	Yes
Network intrusion prevention	Yes	Yes
Browser intrusion prevention	Yes • Log-only mode	No
Excluded hosts (network intrusion prevention)	Yes	Yes

**You can set up the Apache web server that installs with Symantec Endpoint Protection Manager as a reverse proxy for LiveUpdate content.

For more information, see:

- [Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy](#)
- [Managing intrusion prevention](#)

Table 218: Memory Exploit Mitigation policy settings based on platform

Policy setting	Windows	Mac
Memory Exploit Mitigation	Yes • Fine-tuning false positives • Custom applications (cloud only)	No

For more information, see:

[Hardening Windows clients against memory tampering attacks with a Memory Exploit Mitigation policy](#)

LiveUpdate policy settings based on platform

Table 219: LiveUpdate policy settings based on platform

Policy setting	Windows	Mac	Linux
Use the default management server	Yes	No **	No **
Use a LiveUpdate server (internal or external)	Yes	Yes	Yes
Use a Group Update Provider	Yes	No	No
Enable third-party content management	Yes	No	No
Enable/disable definitions	Yes	Yes	No
Reduced-size definitions	Yes	No	No
Run Intelligent Updater to update content	- Virus and spyware definitions - Behavioral analysis (SONAR) - IPS definitions	Virus and spyware definitions	Virus and spyware definitions
LiveUpdate proxy configuration	Yes	Yes, but it is not configured in the LiveUpdate policy. To configure this setting, click Clients > Policies , and then click External Communications Settings .	Yes
LiveUpdate schedule settings	- Frequency - Retry window - Download randomization - Run when computer is idle - Options for skipping LiveUpdate	- Frequency - Download randomization	- Frequency - Retry window - Download randomization
Client security patches	Yes	No	No
Application control content	Yes (14.2)	No	No

** You can set up the Apache web server that installs with Symantec Endpoint Protection Manager as a reverse proxy for LiveUpdate content.

For more information, see:

- [Enabling Mac and Linux clients to download LiveUpdate content using the Apache Web server as a reverse proxy](#)
- [How to choose a client installation type](#)
- [How to update content and definitions on the clients](#)
- [Using Intelligent Updater files to update content on Symantec Endpoint Protection clients](#)

Web and Cloud Access Protection policy settings based on platform

Policy setting	Windows	Mac	Linux
PAC File method Local Proxy Service	Yes	Yes (14.2 RU2 and later)	No
Tunnel method (14.3 RU1)	Yes, Windows 10 64-bit and later only	No	No

For more information, see:

[Controlling Internet access with Web and Cloud Access Protection](#)

Exceptions policy settings based on platform

Table 220: Exceptions policy settings based on platform

Policy setting	Windows	Mac	Linux
Server-based exceptions	• Applications • Applications to monitor • Extensions • Files • Folders • Known risks • Trusted web domains • Tamper Protection exceptions • DNS or Host file change exceptions • Certificate	• Security risk exceptions for files or folders	• Folders • Extensions
Client restrictions (Controls which restrictions end users can add on the client computer)	Yes	No	No

For more information, see:

[Managing exceptions in Symantec Endpoint Protection](#)

Device Control differences based on platform

Application control runs on Windows computers only.

Table 221: Device Control differences based on platform

Windows	Mac
Device control works based only on Class ID (GUID) and Device ID.	Device control works at the file system level. Volume-level tasks (such as those that can be performed via command line or Disk Utility) are unaffected.
Device control performs wildcard matches on Class ID or Device ID with the star character or asterisk (*).	Device control performs regular expression (regexp) matches, and are limited to the following specific operations: • . (dot) • \ (backslash) • [set], [^Set] (set) • * (star character or asterisk) • + (plus)

Windows	Mac
The Hardware Device list includes many common device types by default.	You can choose from only five device types: • Thunderbolt • CD/DVD • USB • FireWire • Secure Digital (SD) Card You do not use the Hardware Device list.
You can add additional custom devices to the Hardware Device list by Class ID or Device ID.	You cannot add additional custom devices.
Devices to block (or to exclude from blocking) are derived only from the Hardware Device list. The list includes those default common device types, as well as custom devices you may have added.	Devices to block (or exclude from blocking) are selected from the device types noted above. The vendor, model, and serial number can be left blank, or can be defined by regular expression (regexp) queries. You can use regular expressions to define a range of similar devices, such as from different vendors, model, serial number ranges, and so on.
You can add more than one device type at a time.	You can only add one device type at a time.
The actions to take are to block, or to exclude from blocking (allow).	The actions to take are to block, or to exclude from blocking (allow) with mount permissions. The following mount permissions are supported: • Read only • Read and write • Read and execute • Read, write, and execute
You can customize the client notification for device control.	You cannot customize the client notifications for device control.

For more information, see:

[Managing device control](#)

Symantec Endpoint Protection feature dependencies for Windows clients

Some policy features require each other to provide complete protection on Windows client computers.

WARNING

Symantec recommends that you do not disable Insight lookups.

Table 222: Dependencies of protection features

Feature	Interoperability Notes
Download Protection	Download Protection is part of Auto-Protect and gives Symantec Endpoint Protection the ability to track URLs. The URL tracking is required for several policy features. If you install Symantec Endpoint Protection without Download Protection, Download Insight has limited capability. Browser Intrusion Prevention requires Download Protection. The Automatically trust any file downloaded from an intranet website option also requires Download Protection.
Download Insight	Download Insight has the following dependencies: • Auto-Protect must be enabled If you disable Auto-Protect, Download Insight cannot function even if Download Insight is enabled. • Insight lookups must be enabled Symantec recommends that you keep the Insight lookups option enabled. If you disable the option, you disable Download Insight completely. Note: If basic Download Protection is not installed, Download Insight runs on the client at level 1. Any level that you set in the policy is not applied. The user also cannot adjust the sensitivity level. Even if you disable Download Insight, the Automatically trust any file downloaded from an intranet website option continues to function. If you disable Download Insight, you disable portal detections. This means that Auto-Protect and scheduled and on-demand scans evaluate all files as non-portal files and use a sensitivity level that is determined by Symantec. See: Managing Download Insight detections
Insight Lookup and cloud protection	Insight Lookup uses the Symantec Insight reputation database in the cloud to make decisions about files that were downloaded from a supported portal. The Insight Lookup functionality runs automatically as part of Auto-Protect, scheduled scans, and on-demand scans on standard and embedded/VDI clients. The standard and embedded/VDI clients support cloud-enabled content. For more information, see: How Windows clients receive definitions from the cloud Cloud scans have the following feature dependencies: • Insight lookups must be enabled. Otherwise, cloud scans and Insight Lookup cannot function. • Download Insight must be enabled so that files can be marked as portal files. • If Download Insight is disabled, cloud scans and Insight Lookup continue to function. They use a sensitivity level that is automatically set by Symantec that detects only the most malicious files.
SONAR	SONAR has the following dependencies: • Download Protection must be installed. • Auto-Protect must be enabled. If Auto-Protect is disabled, SONAR loses some detection functionality and appears to malfunction on the client. SONAR can detect heuristic threats, however, even if Auto-Protect is disabled. • Insight lookups must be enabled. Without Insight lookups, SONAR can run but cannot make detections. In some rare cases, SONAR can make detections without Insight lookups. If Symantec Endpoint Protection has previously cached reputation information about particular files, SONAR might use the cached information. For more information, see: Managing SONAR
Browser Intrusion Prevention	Download Protection must be installed. Download Insight can be enabled or disabled.

Feature	Interoperability Notes
Trusted Web Domain exception	The exception is only applied if Download Protection is installed.
Custom IPS signatures	Uses the firewall. See: Managing custom intrusion prevention signatures
Power Eraser	Uses Insight lookups. Power Eraser uses reputation information to examine files. Power Eraser has a default reputation sensitivity setting that you cannot modify. If you disable the option Allow Insight lookups for threat detection , Power Eraser cannot use reputation information from Symantec Insight. Without Insight, Power Eraser makes fewer detections, and the detections are more likely to be false positives. Note: Power Eraser uses its own reputation thresholds that are not configurable in Symantec Endpoint Protection Manager. Power Eraser does not use the Download Insight settings. For more information, see: What you should know before you run Power Eraser from the Symantec Endpoint Protection Manager console
Memory Exploit Mitigation	Intrusion prevention must be installed. Intrusion prevention can be enabled or disabled.

More information

[Choosing which security features to install on the client](#)

Tools that are included with Symantec Endpoint Protection

This article describes the tools that are included with Symantec Endpoint Protection and what you use the tools for.

- [Tools that are located on the installation file](#)
- [Tools that are installed with Symantec Endpoint Protection Manager](#)
- [Tools attached to a Knowledge Base \(KB\) article](#)

Tools that are located on the installation file

The following tools and documentation are located in the \Tools folder of the full Symantec Endpoint Protection installation file that you download from the Broadcom [Download Management](#) page. To view the Tools folder, extract the full Symantec Endpoint Protection using a tool such as 7-zip.

You can find many of the Help files for these tools in the tools zip file at:

[Related Documents](#)

ApacheReverseProxy

This tool sets up the Apache webserver in Symantec Endpoint Protection Manager to allow Mac clients and Linux clients to download LiveUpdate content through the web server. The Apache webserver works with the Symantec Endpoint Protection Manager to download and cache the LiveUpdate content for Mac and Linux clients locally whenever new content is published.

This tool is appropriate for networks with a smaller number of clients.

CleanWipe

CleanWipe uninstalls the Symantec Endpoint Protection product. Only use CleanWipe as a last resort after you have unsuccessfully tried other uninstallation methods, such as the Windows Control Panel.

You can also find this tool in the following location: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

See also: [Uninstall Symantec Endpoint Protection](#)

ContentDistributionMonitor (SEPMMonitor)

The Content Distribution Monitor helps monitor Group Update Provider (GUP) health and status as well as general content deployment. This tool is a lightweight, standalone tool designed to be run directly on the Symantec Endpoint Protection Manager (SEPM) server, and should return a graphical display of the content distribution status.

Deception

Deception is used to detect adversary activity at the endpoint using "deceptors." The underlying assumption with this approach is that the attacker has already breached the primary defenses of the network and performs reconnaissance in the environment. The attacker looks to find critical assets, like a domain controller or database credentials.

DeviceInfo

DeviceInfo obtains the device vendor, model, or serial number for a specific Mac device. You add this information to the **Hardware Devices** list. You can then add the device ID to a Device Control policy to allow or block a device on client computers.

More information

- [Obtaining a device vendor, model, or serial number for Mac devices with DeviceInfo](#)
- [Mac Device Control in Endpoint Protection](#)
- [Adding hardware devices to the Hardware Devices list](#)
- [Blocking or allowing devices using Device Control and Application Control](#)

ITAnalytics

The IT Analytics software expands the built-in reporting that Symantec Endpoint Protection offers by enabling you to create custom reports and custom queries. It brings multi-dimensional analysis and graphical reporting features from the data that is contained within the Symantec Endpoint Protection Manager databases. This functionality allows you to explore data on your own, without advanced knowledge of databases or third-party reporting tools.

JAWS

The JAWS screen reader program and a set of scripts make it easier to read the Symantec Endpoint Protection menus and dialogs. JAWS is an assistive technology that provides compliance with Section 508 product accessibility.

No Support

- **MoveClient**

`MoveClient` is a Visual Basic script that moves clients from one Symantec Endpoint Protection Manager group to another group based on the client's host name, user name, IP address, or operating system. It also can switch clients from user mode to computer mode and vice versa. See:

[Switching a Windows client between user mode and computer mode](#)

- **Qextract**

`Qextract` extracts and restores files from the client's local quarantine. You might need this tool if the client quarantines a file that you determine is a false positive.

PushDeploymentWizard

You use the Push Deployment Wizard to deploy the Symantec Endpoint Protection client installation package to target computers. Push Deployment Wizard is the same as the Client Deployment Wizard in Symantec Endpoint Protection Manager. You typically use it to deploy to smaller groups of computers or remote computers. See:

For more information, see: [Overview of the Push Deployment Wizard in Symantec Endpoint Protection](#)

SylinkDrop

In 14.3 RU5 and later, the SylinkDrop tool is [installed with the Symantec Endpoint Protection Manager only](#).

SymDiag

SymDiag is a multi-product diagnostic tool that identifies common issues, gathers data for support-assisted troubleshooting, and provides links to other customer self-help and support resources. SymDiag also provides licensing and maintenance status for some Symantec products as well as the Threat Analysis Scan, which helps to find potential malware.

Virtualization

The virtualization tools improve scan performance for the clients that are installed in virtual desktop infrastructure (VDI) environments.

- **SharedInsightCache**

The Shared Insight Cache tool improves scan performance in virtualized environments by not scanning the files that a Symantec Endpoint Protection client has determined are clean. When the client scans a file for threats and determines it is clean, the client submits information about the file to Shared Insight Cache.

When another client subsequently attempts to scan the same file, that client can query Shared Insight Cache to determine if the file is clean. If the file is clean, the client does not scan that particular file. If the file is not clean, the client scans the file for viruses and submits those results to Shared Insight Cache.

Shared Insight Cache is a web service that runs independently of the client. However, Symantec Endpoint Protection must be configured to specify the location of Shared Insight Cache so that the clients can communicate with it. Shared Insight Cache communicates with the clients through HTTP or HTTPS. The client's HTTP connection is maintained until the scan is finished. See:

[Installation and Configuration of SEP Shared Insight Cache](#)

- **Virtual Image Exception**

To increase performance and security in a VDI environment, a common practice is to leverage base images to build virtual machine sessions as needed. The Symantec Virtual Image Exception tool lets Symantec Endpoint Protection clients bypass scanning base image files for threats, which reduces the resource load on disk I/O. It also improves CPU scanning process performance in a VDI environment. See:

[About the Symantec Virtual Image Exception tool](#)

WebServicesDocumentation

Symantec Endpoint Protection includes a set of public APIs in the form of web services to provide support for remote monitoring and management (RMM) applications. The web services provide functions on the client and on the management server. All calls to Symantec Endpoint Protection web services are authenticated using OAuth and allow access only by authorized Symantec Endpoint Protection administrators. Developers use these APIs to integrate their company's third-party network security solution with the Symantec Endpoint Protection management server and client.

Provides the support for remote management and remote monitoring. Remote management is provided by means of public APIs in the form of web services that let you integrate your third-party solution or custom console with basic client and management server functionality. Remote monitoring is provided by means of publicly supported registry keys and Windows event logging.

Web services for remote management can do the following tasks:

- Reports the license status and content status on the management server by web service calls, in addition to reporting the license status to the Windows Event Log.
- Issues commands to the client, such as Update, Update and Scan, and Restart.
- Manages the policies that are delivered to the client. Policies can be imported from another management server, and they can be assigned to groups or locations at another management server.

Tools that are installed with Symantec Endpoint Protection Manager

The following tools are installed with the Symantec Endpoint Protection Manager in the following default location: C:

\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

CleanWipe

CollectLog

CollectLog.cmd places the Symantec Endpoint Protection Manager logs in a compressed .zip file. You send the .zip file to Broadcom Support or another administrator for troubleshooting purposes.

ConfigSEPM

In some secure or isolated environments, you may need to disable all outbound connections from the Symantec Endpoint Protection Manager to the Internet.

See: [How to disable all outbound network connections from the Endpoint Protection Manager](#)

Database Validator

You use dbvalidator.bat to help Support diagnose a problem with the database that Symantec Endpoint Protection Manager runs.

LogUtils

scm-datacollector

Used to create memory and thread dumps due to the difficulty of using virtual service accounts (VSAs) with more secure permissions and privileges.

See: [SEPM troubleshooting data collector](#)

SetSQLServerTLSEncryption

Symantec Endpoint Protection Manager communicates with the Microsoft SQL Server over an encrypted channel by default. This tool lets you disable or enable TLS encryption between the management server and the Microsoft SQL Server communication. As of version 14, it can be used with the management server installations that are configured to use the Microsoft SQL Server database.

SylinkDrop

The Sylink.xml file includes communication settings between the Windows client and a Symantec Endpoint Protection Manager. If the clients have lost the communication with Symantec Endpoint Protection Manager, use the SylinkDrop tool to automatically replace the existing Sylink.xml file with a new Sylink.xml file on the client computer.

Replacing the Sylink.xml file does the following tasks:

- Converts an unmanaged client to a managed client.
- Migrates or moves clients to a new domain or management server.
- Restores the communication breakages to the client that cannot be corrected on the management server.
- Moves a client from one server to another server that is not a replication partner.
- Moves a client from one domain to another.

You can also use this tool for Windows clients only; the tool is located in the following location (64-bit): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

For more information, see:

[Restoring client-server communication settings by using the SylinkDrop tool](#)

Third-party removal tool (TPAR)

Removes third-party security software on the client computer so that you can install the Symantec Endpoint Protection client.

See: [Third-party security software removal in Endpoint Protection/Endpoint Security](#)

updatedbtime

See: [SEPM LiveUpdate is not functioning after the server's clock was accidentally moved into the future](#)

Tools attached to a Knowledge Base (KB) article

Download each tool either from within the article or at the bottom in the attachments section.

API reference

Symantec Endpoint Protection Manager includes a set of REST APIs that connect to and perform Symantec Endpoint Protection Manager operations from Endpoint Detection and Response (EDR). You use the APIs if you do not have access to Symantec Endpoint Protection Manager. The documentation is located in the following places:

- The Broadcom portal. See:
[Endpoint Security REST API Documentation](#)
- On the Symantec Endpoint Protection Manager server at the following address, where SEPM-IP is the IP address of the Symantec Endpoint Protection Manager server:
`https://SEPM-IP:8446/sepm/restapidocs.html`
IP address includes IPv4 and IPv6. You must enclose the IPv6 address with square brackets: `http://[SEPM-Server]:port number`

CleanWipe

See: [Uninstall Symantec Endpoint Protection](#)

Database Schema

Call Broadcom Technical Support, who can provide the Symantec Endpoint Protection Manager schema.

DeviceInfo

DevViewer obtains the device vendor, model, or serial number for a specific Windows device. You add this information to the **Hardware Devices** list in the Symantec Endpoint Protection Manager. You can then add the GUID or the device ID to a Device Control policy to allow or block a device on client computers.

Download DevViewer from the Attachments section at:

[Use DevViewer to find hardware device IDs for Device Blocking in Endpoint Protection](#)

More information

- [Adding a hardware device to the Hardware Devices list](#)
- [Block or allow devices in Endpoint Protection](#)

LiveUpdate Administrator

Symantec LiveUpdate Administrator is a standalone web application that is separate from Symantec Endpoint Protection. LiveUpdate Administrator mirrors the content of the public LiveUpdate servers and then offers the content to Symantec products internally through a built-in web server.

LiveUpdate Administrator is an optional component for Symantec Endpoint Protection and is not required to update the Symantec Endpoint Protection clients. By default, the Symantec Endpoint Protection Manager uses the LiveUpdate technology rather than LiveUpdate Administrator to download contents directly from the Symantec public LiveUpdate servers.

You may want to use LiveUpdate Administrator in some circumstances. For example, you may need to download content to a large number of non-Windows clients or to clients if Symantec Endpoint Protection Manager cannot download the content. Therefore, you can install a LiveUpdate Administrator server and then configure the Symantec Endpoint Protection Manager to download from it. See:

[When to use LiveUpdate Administrator](#)

To download LiveUpdate Administrator and the documentation, see:

- [Download LiveUpdate Administrator \(LUA\)](#)
- [LiveUpdate Administrator release notes and fix notes](#)

Commands for the Windows client service smc in Symantec Endpoint Protection and Symantec Endpoint Security

You can run the Windows client service using the `smc` (or `smc.exe`) command-line interface. You can use the `smc` command in a script that runs the client remotely. For example, you may need to stop the client to install an application on multiple clients. You can then use the script to stop and restart all clients at one time.

The client service must be running for you to use the command-line parameters, with the exception of `smc -start` parameter. The command-line parameters are not case-sensitive. For some parameters, you may need the password. The client does not support UNC paths.

To run Windows commands using the `smc` command-line interface

1. On the client computer, click **Start > Run**, and then type `cmd`.
2. In the Command Prompt window, do one of the following tasks:

- If the parameter does not need a password, enter:

```
smc -parameter
```

Where parameter is a parameter.

- If the parameter needs a password, enter:

- `smc -password -parameter`

For example: `smc -password -exportconfig c:\profile.xml`

NOTE

You must enter the installation path to the `smc` service before the command. For example, on a 64-bit Windows system on which Symantec Endpoint Protection is installed to the default location, enter:

```
C:\Program Files\Symantec\Symantec Endpoint Protection\smc.exe
```

Table 223: Parameters for `smc`

Parameter	Description	Applies to
<code>smc -start *</code>	Starts the client service. Returns 0, -1	All supported versions
<code>smc -stop *†</code>	Stops the client service and unloads it from memory. If this command is password-protected, the client is disabled within one minute after the end user enters the correct password. Returns 0, -1	All supported versions
<code>smc -cloudmanaged <path to Symantec_Agent_Setup></code>	Moves a cloud-managed device to another cloud domain or tenant. Moves a client computer from Symantec Endpoint Protection Manager management to cloud console management. Requires the <code>Symantec_Agent_Setup.exe</code> installation file for the destination cloud domain or tenant. You download this file from the cloud console. See: Using smc to switch Windows client between SEP and SES management or to change a device's tenant or domain	New in 14.2 RU1

Parameter	Description	Applies to
<code>smc -configure -proxy-mode <mode></code>	Used together with enrollment parameters to enable the client to enroll using the required proxy configuration. Can also be used to correct bad proxy options. Possible modes are as follows: system , manual , none . Specifying a proxy address switches automatically to manual mode. If you enter manual , but don't specify a proxy host, this mode will be ignored. Not supported on the clients that are managed by Symantec Endpoint Protection Manager. For more information, see the table: Combinations of proxy settings entered at a command prompt	New in 14.3 RU1
<code>smc -configure -proxy-address <host or IP></code>	Allows to manually specify the proxy host or the proxy address. Required if the proxy mode is set to manual .	New in 14.3 RU1
<code>smc -configure -proxy-port <port number></code>	Allows to manually specify the proxy port. The same port will be used both for HTTP and HTTPS connections. If no ports are specified, the ports are automatically set to 80 for HTTP and 443 for HTTPS.	New in 14.3 RU1
<code>smc -configure -proxy-port-http <port number></code>	Allows to manually specify the proxy port for HTTP connections. Overwrites the default HTTP port or the port that has been specified by <code>smc -configure -proxy-port</code> .	New in 14.3 RU1
<code>smc -configure -proxy-port-https <port number></code>	Allows to manually specify the proxy port for HTTPS connections. Overwrites the default HTTPS port or the port that has been specified by <code>smc -configure -proxy-port</code> .	New in 14.3 RU1
<code>smc -configure -proxy-auth-mode basic</code>	Possible authentication modes are as follows: basic , ntlm . Default authentication mode is basic .	New in 14.3 RU1
<code>smc.exe -configure -proxy-user-name <name></code>	Allows to manually specify the proxy user. For ntlm , you must specify domain/user.	New in 14.3 RU1
<code>smc -configure -proxy-password <plain pwd></code>	Allows to manually specify the proxy password. Maximum length is 255 characters without null. The password is case sensitive.	New in 14.3 RU1
<code>smc -enable -ntp</code> <code>smc -disable -ntp †</code>	Enables/disables the Symantec Endpoint Protection firewall and Intrusion Prevention System.	All supported versions Password requirement for <code>-disable</code> new in 14.2 RU1
<code>smc -enable -mem *</code> <code>smc -disable -mem *</code>	Enables/disables the Symantec Endpoint Protection Memory Exploit Mitigation system.	New in version 14 MP1
<code>smc -enable -gem *</code> <code>smc -disable -gem *</code>	Enables/disables the Symantec Endpoint Protection Memory Exploit Mitigation system.	Version 14 only
<code>smc -dismissgui</code>	Closes the client user interface. The client still runs and protects the client computer. Returns 0	All supported versions

Parameter	Description	Applies to
<code>smc -exportconfig *†</code>	Exports the client's configuration file to an .xml file. The configuration file includes the following management server settings: • Policies • Groups • Security settings • User interface settings You must specify the path name and file name. For example, you can enter the following command: <pre>smc -exportconfig C:\My Documents\MyCompanyprofile.xml</pre> Returns 0, -1, -5, -6	All supported versions
<code>smc -exportlog</code>	Exports the entire contents of a log to a .txt file. To export a log, you use the following syntax: <pre>smc -exportlog log_type 0 -1 output_file</pre> Where: log_type is: • 0 = System Log • 1 = Security Log • 2 = Traffic Log • 3 = Packet Log • 4 = Control Log For example, you might enter the following syntax: <pre>smc -exportlog 2 0 -1 c:\temp\TrafficLog</pre> Where 0 is the beginning of the file and -1 is the end of the file. You can export only the Control log, Packet log, Security log, System log, and Traffic log. The name output_file is the path name and file name that you assign to the exported file. Returns 0, -2, -5	All supported versions
<code>smc -exportadvrule *†</code>	Exports the client's firewall rules to an .xml file. This command only works for firewall rules on an unmanaged client or a client that is in client control mode. For a client in server control mode or mixed mode, use <code>-exportconfig</code>. You must specify the path name and file name. For example, you can enter the following command: <pre>smc -exportadvrule C:\myrules.xml</pre> Returns 0, -1, -5, -6 You cannot import configuration files or firewall rule files directly from a mapped network drive. Preventing users from disabling the Symantec Endpoint Protection client	All supported versions
<code>smc -image †</code>	Unenrolls the Symantec Agent (Symantec Endpoint Protection client) and keeps it unenrolled. The difference from a regular unenrollment is the removal of the hardware key and the persisted hardware key information. Uses the Require a password to import or export a policy and to import client communication settings password option. For clients that the SES cloud console manages, running the <code>smc -image</code> command also results in the client becoming unmanaged. You would then need to run another command to re-register the client with its cloud server. See: Installing Symantec Agent on a client device without automatically enrolling it	New in 14.3 RU1 (Symantec Endpoint Security) New in 14.3 RU6 (Symantec Endpoint Protection)

Parameter	Description	Applies to
<code>smc -importadvrule *†</code>	Imports the firewall rules to the client. The rules you import overwrite any existing rules. You can import the following: - Rules in .xml format that you exported through <code>smc -exportadvrule</code> - Rules in .sar format that you exported through the client user interface You can only import firewall rules if the client is unmanaged or if the managed client is in client control mode or mixed mode. The managed client ignores these rules in server control mode. To import firewall rules, you import an .xml or .sar file. For example, you can enter the following command: <pre>smc -importadvrule C:\myrules.xml</pre> An entry is added to the System log after you import the rules. Returns 0, -1, -5, -6 To append rules instead of overwriting them, use Import rule from the within client user interface. For more information, see: Preventing and allowing users to change the client's user interface Exporting or importing firewall rules on the client	All supported versions
<code>smc -importconfig *†</code>	Replaces the contents of the client's current configuration file with an imported configuration file and updates the client's policy. The client must run to import the configuration file's contents. You must specify the path name and file name. For example, you can enter the following command: <pre>smc -importconfig C:\My Documents\MyCompanyprofile.xml.</pre> Returns 0, 3, -1, -5, -6	All supported versions
<code>smc -importsymlink <path to symlink.xml>†</code>	Imports the client communications file (symlink.xml).	All supported versions
<code>smc -enable -wss</code> <code>smc -disable -wss</code>	Enables or disables Web and Cloud Access Protection.	New in version 14.0.1 MP1
<code>smc -p password†</code>	Used with a command that requires a password, where password is the required password. For example: <pre>smc -p password -importconfig</pre>	All supported versions
<code>smc -report</code>	Creates a dump file (.dmp) that includes crashes and logical errors that occurred on the client. The file is sent automatically to Symantec Technical Support. Contact Technical Support to ask for help in diagnosing the error. You can find the dump file at the following location: <pre>SEP_Install\Data\LocalDumps</pre> Where SEP_Install is the installation folder. By default, this path is C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\version.	New in version 14
<code>smc -restart</code>	Stops and immediately starts the client, which performs the same task as <code>-stop</code> followed by <code>-start</code> . The command restarts the client without restarting the computer. Use this command as a troubleshooting tool to help diagnose an unknown problem.	New in 14.3 RU3
<code>smc -runhi</code>	Runs a Host Integrity check. Returns 0	All supported versions
<code>smc -sepmmanaged</code>	Reverts the client management from the cloud console back to the Symantec Endpoint Protection Manager that previously managed it.	New in 14.2 RU1

Parameter	Description	Applies to
<code>smc -sepmmanaged <path to sylink.xml></code>	Imports the client communications file (sylink.xml). Equivalent to <code>-importsylink</code> but does not require a password.	New in 14.2 RU1
<code>smc -showgui</code>	Displays the client user interface. Returns 0	All supported versions
<code>smc -updateconfig</code>	Initiates a client-server communication to ensure that the client's configuration file is up-to-date. If the client's configuration file is out-of-date, <code>updateconfig</code> downloads the most recent configuration file and replaces the existing configuration file, which is <code>serdef.dat</code> . Returns 0	All supported versions

`smc -checkinstallation` and `smc -checkrunning` are no longer supported.

* Parameters that only members of the Administrators group can use if the following conditions are met:

- The client runs Windows Vista or Windows Server 2008, and users are members of the Windows Administrators group.
If the client runs Windows Vista, and User Account Control is enabled, the user automatically becomes a member of the groups Administrators and Users.

† Parameters that need a password. You password-protect the client in Symantec Endpoint Protection Manager.

See: [Password-protecting the Symantec Endpoint Protection client](#)

Table 224: Combinations of proxy settings entered at a command prompt

proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	Action
system	no	no	no	no	Use system proxy
system	yes	no	no	no	ERROR_INVALID_COMMAND_LINE (missing password)
system	no	yes	no	no	ERROR_INVALID_COMMAND_LINE (missing user)
system	no	no	yes	no	Use system proxy (ignore server)
system	yes	yes	no	no	Use system proxy with authentication
system	yes	yes	yes	no	Use system proxy with authentication (ignore server)
system	yes	yes	yes	yes	Use system proxy with authentication (ignore server and ports)
manual	no	no	no	no	ERROR_INVALID_COMMAND_LINE
manual	yes	no	no	no	ERROR_INVALID_COMMAND_LINE
manual	no	yes	no	no	ERROR_INVALID_COMMAND_LINE
manual	no	no	yes	no	Valid "manual" (custom) proxy with default ports
manual	yes	yes	no	no	ERROR_INVALID_COMMAND_LINE
manual	yes	yes	yes	no	Valid "manual" (custom) proxy with default ports
manual	yes	yes	yes	yes	Valid "manual" (custom) proxy

proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	Action
manual	yes	no	yes	yes or no	ERROR_INVALID_COMMAND_LINE (no password)
manual	no	yes	yes	yes or no	ERROR_INVALID_COMMAND_LINE (no user)
none	no	no	no	no	Valid "none" proxy
none	yes	no	no	no	Valid "none" proxy
none	no	yes	no	no	Valid "none" proxy
none	no	no	yes	no	Valid "none" proxy
none	yes	yes	no	no	Valid "none" proxy
none	yes	yes	yes	no	Valid "none" proxy
none	yes	yes	yes	yes	Valid "none" proxy
no	no	no	no	no	No proxy settings
no	yes	no	no	no	No proxy settings (ignore user)
no	no	yes	no	no	No proxy settings (ignore password)
no	no	no	yes	no	Valid "manual" (custom) proxy with default ports
no	yes	yes	no	no	No proxy settings (ignore extra options)
no	yes	yes	yes	no	Valid "manual" (custom) proxy with default ports
no	yes	yes	yes	yes	Valid "manual" (custom) proxy

More information

[command error codes](#)

smc.exe command error codes

The following table displays the error codes that the `smc.exe` command returns when the required parameters are invalid or missing.

Table 225: smc.exe command error codes

Error code	Description
0	Command was successful.
-1	User is not in the Windows Administrators or Windows Power Users group. If the client runs Windows Vista, the user is not a member of the Windows Administrators group.
-2	Invalid parameter. You may have typed the parameter incorrectly, or you may have added an incorrect switch after the parameter.
-3	smc client service is not installed.
-4	smc client service is not running.

Error code	Description
-5	Invalid input file. For example, the <code>importconfig</code> , <code>exportconfig</code> , <code>updateconfig</code> , <code>importadv</code> , <code>exportadvrule</code> , and <code>exportlog</code> parameters require the correct path name and file name.
-6	Input file does not exist. For example, the <code>importconfig</code> , <code>updateconfig</code> , and <code>importadvrule</code> parameters require the correct path name, configuration file name (.xml) or firewall rules file name (.sar).

More information

[Windows commands for the Endpoint Protection client service](#)

Installing Windows client software using third-party tools

You can install the client using third-party tools instead of the tools that are installed with the management server. If you have a large network, you are more likely to benefit by using these options to install Symantec client software.

You can install the client by using a variety of third-party products. These products include Microsoft Active Directory, Tivoli, Microsoft Systems Management Server (SMS), and Novell ZENworks. Symantec Endpoint Protection supports Novell ZENworks, Microsoft Active Directory, and Microsoft SMS.

You can also deploy Symantec Endpoint Protection in an environment that you manage with a **Symantec Software Management Solution powered by Altiris**. You can deploy Symantec Endpoint Protection from one of the Software Management Solution suites with one of the following policies:

- A **Managed Software Delivery** policy
- A **Quick Delivery** policy

For more information, refer to the Software Management Solution suite product Help, or see:

[Symantec Software Management Solution product landing page](#)

Table 226: Third-party tools to install the client

Tool	Description
Windows Installer command-line tools	The Symantec client software installation packages are Windows Installer (MSI) files that you can configure by using the standard Windows Installer options. You can use the environment management tools that support MSI deployment, such as Active Directory or Tivoli, to install clients on your network. You can configure how the Windows Security Center interacts with the unmanaged client. See: • About client installation features and properties • About configuring MSI command strings • About configuring Setaid.ini • Symantec Endpoint Protection command-line client features • Symantec Endpoint Protection command-line client installation properties • Windows Installer parameters • Command-line examples for installing the Windows client • Windows Security Center properties
Microsoft SMS 2003	You can install the client by using Microsoft Systems Management Server. See: Installing Windows clients with Microsoft SCCM/SMS

Tool	Description
Windows Active Directory	You can use a Windows Active Directory Group Policy Object if the client computers are members of a Windows Active Directory domain. The client computers must also use a supported Windows operating system. See: • Installing Windows clients with an Active Directory Group Policy Object (GPO) • Uninstalling client software with an Active Directory Group Policy Object
Virtualization software	You can install the client in virtual environments. See: Supported virtual installations and virtualization products

More information

[Exporting client installation packages](#)

About client installation features and properties

Installation features and properties appear as strings in text files and command lines. Text files and command lines are processed during all client software installations. Installation features control which components get installed. Installation properties control which subcomponents are enabled or disabled after installation. Installation features and properties are available for Symantec Endpoint Protection client software only and are also available for the Windows operating system. Installation features and properties are not available for the installation of Symantec Endpoint Protection Manager.

Installation features and properties are specified in the following ways: as lines in the Setaid.ini file and as values in Windows Installer (MSI) commands. MSI commands can be specified in Windows Installer strings and in Setaid.ini for a customized deployment. Windows Installer commands and Setaid.ini are always processed for all managed client software installations. If different values are specified, the values in Setaid.ini always take precedence.

About configuring MSI command strings

Symantec Endpoint Protection installation software uses Windows Installer (MSI) 3.1 or later packages for installation and deployment. If you use the command line to deploy a package, you can customize the installation. You can use the standard Windows Installer parameters and the Symantec-specific features and properties.

To use the Windows Installer, elevated privileges are required. If you try the installation without elevated privileges, the installation may fail without notice.

For the most up-to-date list of Symantec installation commands and parameters, see the article:

[MSI command line reference for Symantec Endpoint Protection.](#)

NOTE

The Windows Installer advertise function is unsupported. Setaid.ini-specified features and properties take precedence over MSI-specified features and properties. Feature and property names in MSI commands are case-sensitive. See:

[About configuring Setaid.ini](#)

About configuring Setaid.ini

Setaid.ini appears in all installation packages and controls many of the aspects of the installation, such as which features are installed. Setaid.ini always takes precedence over any setting that may appear in an MSI command string that is used to start the installation. Setaid.ini appears in the same directory as setup.exe. If you export to a single .exe file, you cannot configure Setaid.ini. However, the file is automatically configured when you export Symantec Endpoint Protection client installation files from the console.

The following lines show some of the options that you can configure in Setaid.ini.

```
[CUSTOM_SMC_CONFIG]
InstallationLogDir=
DestinationDirectory=

[FEATURE_SELECTION]
Core=1

SAVMain=1
  Download=1
  OutlookSnapin=1
  Pop3Smtplib=0
  NotesSnapin=0

PTPMain=1
  DCMain=1
  TruScan=1
```

NOTE

The features are indented to show hierarchy. The features are not indented inside the Setaid.ini file. Feature names in Setaid.ini are case-sensitive.

Feature values that are set to 1 install the features. Feature values that are set to 0 do not install the features. You must specify and install the parent features to successfully install the client features.

Be aware of the following additional setaid.ini settings that map to MSI properties for Symantec Endpoint Protection client installation:

- DestinationDirectory maps to PRODUCTINSTALLDIR
- KeepPreviousSetting maps to MIGRATESETTINGS
- AddProgramIntoStartMenu maps to ADDSTARTMENUICON

More information

- [Symantec Endpoint Protection command-line client features](#)
- [Symantec Endpoint Protection command-line client installation properties](#)
- [Windows Installer parameters](#)

Symantec Endpoint Protection command-line client installation properties

These installation properties are for use with MSI command line installations.

Table 227: Symantec Endpoint Protection client installation properties

Property	Description
RUNLIVEUPDATE=val	Determines whether LiveUpdate is run as part of the installation, where val is one of the following values: 1: Runs LiveUpdate during installation (default). 0: Does not run LiveUpdate during installation. By default, all Symantec Endpoint Protection clients in a group receive the latest versions of all content and all product updates. If the clients are configured to get updates from a management server, the clients receive only the updates that the server downloads. If the LiveUpdate Content policy allows all updates, but the management server does not download all updates, the clients receive only what the server downloads.
ENABLEAUTOPROTECT=val	Determines whether File System Auto-Protect is enabled after the installation is complete, where val is one of the following values: 1: Enables Auto-Protect after installation (default). 0: Disables Auto-Protect after installation.
CACHE_INSTALLER=val	Determines whether the installation files cache on the client, where val is one of the following values: 1: Caches the installation files (default). 0: Does not cache the installation files.
MIGRATESETTINGS=val	Determines the status of preserved settings in an upgrade scenario, where val is one of the following values: 0: Does not preserve the settings or logs. 1: Preserves all settings and logs. 2: Preserves Sylink.xml and logs only.
ADDSTARTMENUICON=val	Determines whether or not to add the program to the Start Menu folder, where val is one of the following values: 0: Does not add the program to the Start Menu folder. 1: Adds the program to the Start Menu folder (default).

Installing Symantec Endpoint Protection client features using the command line

You can install the protection features by specifying them in Setaid.ini files and in MSI commands. Most features have a parent-child relationship. If you want to install a child feature that has a parent feature, you must also install the parent feature. For example, if you specify to install the Firewall feature but do not specify to install NTPMain, the firewall is not installed.

NOTE

Application Hardening is disabled unless your Symantec Endpoint Protection Manager domain is enrolled with the Endpoint Security cloud server and the Symantec Endpoint Protection Manager received the Symantec Enterprise Security Complete license.

Table 228: Symantec Endpoint Protection client features

Feature	Description	Required parent features
Core	Installs the files that are used for communications between clients and Symantec Endpoint Protection Manager. This feature is required.	None
ADDefense	Installs the Endpoint Threat Defense for Active Directory component.	Core

Feature	Description	Required parent features
DCMain	Installs the Application Control and Device Control feature.	PTPMMain
Download	Installs the complete protection for downloaded files. Includes fully functional reputation scanning by Download Insight.	SAVMain
Firewall	Installs the firewall feature.	NTPMain
ITPMMain	Installs the Network and Intrusion Prevention and Browser Intrusion Prevention feature.	NTPMain
LANG1033	Installs English resources.	Core
NotesSnapin	Installs the Lotus Notes Auto-Protect email feature. Applies only to versions earlier than 14.2 RU1.	SAVMain
NTPMain	Installs the Network and Host Exploit Mitigation components.	Core
NTR	Installs the Web and Cloud Access Protection component.	Core
OutlookSnapin	Installs the Microsoft Exchange Auto-Protect email feature.	SAVMain
Pop3Smtpp	Installs the protection for POP3 and SMTP mail. Available only on 32-bit systems. Applies to 14.2 RU1 and earlier only.	SAVMain
PTPMMain	Installs the Proactive Threat Protection components.	Core
SAVMain	Installs the virus, spyware, and basic download protection. Subfeatures install additional protection.	Core
TruScan	Installs the Behavioral Analysis (SONAR) feature.	PTPMMain

See: [MSI command line reference for Endpoint Protection](#)

Windows Installer parameters

Symantec Endpoint Protection client installation packages use the standard Windows Installer parameters, as well as a set of extensions for command-line installation and deployment.

See the Windows Installer documentation for further information about the usage of standard Windows Installer parameters. You can also execute `msiexec.exe` from a command line to see the complete list of parameters.

Table 229: Windows Installer parameters

Parameter	Description
Sep.msi (32-bit) Sep64.msi (64-bit)	The installation file for the Symantec Endpoint Protection client. If the file name contains spaces, enclose the file name in quotations when used with <code>/I</code> and <code>/x</code> . Required
Msiexec	Windows Installer executable. Required
/I ".msi file name"	Install the specified file. If the file name contains spaces, enclose the file name in quotations. If the file is not in the same directory from which you execute <code>Msiexec</code> , specify the path name. If the path name contains spaces, enclose the path name in quotations. For example, <code>msiexec.exe /I "C:\path to\Sep.msi"</code> Required
/qn	Install silently.
/x ".msi file name"	Uninstall the specified components. Optional

Parameter	Description
/qb	Install with a basic user interface that shows the installation progress. Optional
/!*v logfilename	Create a verbose log file, where logfilename is the name of the log file you want to create. Optional
PRODUCTINSTALLDIR=path	Designate a custom path on the target computer where path is the specified target directory. If the path includes spaces, enclose the path in quotation marks. By default: 32-bit computers: C:\Program Files\Symantec\Symantec Endpoint Protection 64-bit computers (14.3 RU4 or earlier): C:\Program Files (x86)\Symantec\Symantec Endpoint Protection 64-bit computers (14.3 RU5 or later): C:\Program Files\Symantec\Symantec Endpoint Protection Optional
SYMREBOOT=value	Controls a computer restart after installation, where value is a valid argument. The valid arguments include the following: - Force: Requires that the computer is restarted. Required for uninstallation. - Suppress: Prevents most restarts. - ReallySuppress: Prevents all restarts as part of the installation process, even a silent installation. Optional Note: Use ReallySuppress to suppress a restart when you perform a silent uninstallation of Symantec Endpoint Protection client.
ADDLOCAL= feature	Select the custom features to be installed, where feature is a specified component or list of components. If this property is not used, all applicable features are installed by default, and Auto-Protect email clients are installed only for detected email programs. To add all appropriate features for the client installations, use the ALL command as in ADDLOCAL=ALL. See: Symantec Endpoint Protection command-line client features Note: When you specify a new feature to install, you must include the names of the features that are already installed that you want to keep. If you do not specify the features that you want to keep, Windows Installer removes them. By specifying existing features, you do not overwrite the installed features. To uninstall an existing feature, use the REMOVE command. Optional
REMOVE=feature	Uninstall the previously installed program or a specific feature from the installed program, where feature is one of the following: - Feature: Uninstalls the feature or list of features from the target computer. - ALL: Uninstalls the program and all of the installed features. All is the default if a feature is not specified. Optional

Windows Security Center properties

You can customize Windows Security Center (WSC) properties during Symantec Endpoint Protection client installation. These properties apply to unmanaged clients only. Symantec Endpoint Protection Manager controls these properties for the managed clients.

NOTE

These properties apply to Windows XP Service Pack 3 only. They do not apply to clients that run Windows Vista, or Windows 7 or later, except for the WSCAVUPTODATE property.

Windows Security Center was renamed to Action Center in Windows 7/8 and Security and Maintenance in Windows 10.

Table 230: Windows Security Center properties

Property	Description
WSCCONTROL=val	Controls WSC where val is one of the following values: 0: Do not control (default). 1: Disable one time, the first time it is detected. 2: Disable always. 3: Restore if disabled.
WSCAVALERT=val	Configures the antivirus alerts for WSC where val is one of the following values: 0: Enable. 1: Disable (default). 2: Do not control.
WSCFWALERT=val	Configures the firewall alerts for WSC where val is one of the following values: 0: Enable. 1: Disable (default). 2: Do not control.
WSCAVUPTODATE=val	Configures the WSC out-of-date time for antivirus definitions where val is one of the following values: 1 - 90: Number of days (default is 30).
DISABLEDEFENDER=val	Determines whether to disable Windows Defender during installation, where val is one of the following values: 1: Disables Windows Defender (default). 0: Does not disable Windows Defender.

Command-line examples for installing the Windows client

Table 231: Command-line examples

Task	Command line
Silently install all of the Symantec Endpoint Protection client components with default settings to the directory C:\SFN. Suppress a computer restart, and create a verbose log file.	<code>msiexec /I SEP.msi PRODUCTINSTALLDIR=C:\SFN SYMREBOOT=ReallySuppress /qn /l*v c:\temp\msi.log</code>
Silently install the Symantec Endpoint Protection client with Virus and Spyware Protection, and with intrusion prevention and firewall. Force a computer restart, and create a verbose log file.	<code>msiexec /I SEP.msi ADDLOCAL=Core,SAVMain,OutlookSnapin, Pop3SmtP,ITPMain,Firewall SYMREBOOT=Force /qn / l*v c:\temp\msi.log</code>

Installing Windows clients with Microsoft SCCM/SMS

You can use Microsoft System Center Configuration Manager (SCCM) to install Symantec client software. We assume that system administrators who use SCCM have previously installed software with SCCM. As a result, we assume that you do not need detailed information about installing Symantec client software with SCCM.

NOTE

This topic also applies to Microsoft Systems Management Server (SMS).

NOTE

This note applies to SMS version 2.0 and earlier: If you use SMS, turn off the **Show Status Icon On The Toolbar For All System Activity** feature on the clients in the **Advertised Programs Monitor**. In some

situations, Setup.exe might need to update a shared file that is in use by the Advertised Programs Monitor. If the file is in use, the installation fails.

Symantec recommends that SCCM/SMS packages launch Setup.exe rather than the MSI directly. This method enables installer logging. Use the custom package creation feature in SCCM/SMS to create custom packages instead of the package wizard feature.

WARNING

You should use a managed client installation package that you exported from Symantec Endpoint Protection Manager. If you use the client installation packages from the product download or the installation file, you deploy unmanaged clients. Unmanaged clients install with default settings and do not communicate with a management server. See:

[Installing Symantec Endpoint Protection clients with Save Package](#)

Table 232: Process for installing the client using Microsoft System Center Configuration Manager / Systems Management Server

Step	Description
Step 1	Export a managed client installation package from Symantec Endpoint Protection Manager that contains the software and policies to install on your client computers. By default, a managed client installation package contains a file named Sylink.xml, which identifies the server that manages the clients.
Step 2	Create a source directory and copy the Symantec client installation package into that source directory. For example, you would create a source directory and copy the Setup.exe file that you exported from Symantec Endpoint Protection Manager.
Step 3	In SCCM/SMS, create a custom package, name the package, and identify the source directory as part of the package.
Step 4	Configure the Program dialog box for the package to specify the executable that starts the installation process, and possibly specify the MSI with parameters.
Step 5	Distribute the software to specific Collections with Advertising .

For more information on using SCCM/SMS, see the Microsoft documentation that is appropriate for your version.

Installing Windows clients with an Active Directory Group Policy Object (GPO)

You can install the Windows client by using a Windows Active Directory Group Policy Object. The procedures assume that you have installed this software and use Windows Active Directory to install client software with an Active Directory Group Policy Object.

The Symantec client installation uses standard Windows Installer (MSI) files. As a result, you can customize the client installation with MSI properties. See:

[About configuring MSI command strings](#)

You should confirm that your DNS server is set up correctly before deployment. The correct setup is required because Active Directory relies on your DNS server for computer communication. To test the setup, you can ping the Windows Active Directory computer, and then ping in the opposite direction. Use the fully qualified domain name. The use of the computer name alone does not call for a new DNS lookup. Use the following format:

ping computername.fullyqualifieddomainname.com

WARNING

You should use a managed client installation package that you exported from Symantec Endpoint Protection Manager. If you use the client installation packages from the product download or the installation file, you deploy unmanaged clients. Unmanaged clients install with default settings and do not communicate with a management server. See:

[Installing Symantec Endpoint Protection clients with Save Package](#)

Table 233: Steps for installing the client software by using Active Directory Group Policy Object

Step	Action
Step 1	Export the managed client installation package with the option Separate files (required for .MSI) . See: Installing Symantec Endpoint Protection clients with Save Package
Step 2	Stage the folder of installation files. For example, copy the managed client installation package into a shared folder on which you have set the correct permissions to allow access.
Step 3	Create a GPO software distribution. You should also test GPO installation with a small number of computers before the production deployment. If you do not configure DNS properly, GPO installations can take an hour or more. See: Creating a GPO software distribution
Step 4	Add computers to the organizational unit. See: Adding computers to an organizational unit to install software

More information

[Uninstalling client software with an Active Directory Group Policy Object](#)

Creating a GPO software distribution

If you use Microsoft Active Directory in your environment, you can use a GPO to deploy the Symantec Endpoint Protection client package to Windows computers. You create a software distribution then configure a GPO administrative template for the software packages.

This process assumes that you have installed Microsoft's Group Policy Management Console with Service Pack 1 or later. The Windows interface may be slightly different depending on the version of Windows you use.

This process also assumes that you have computers in the Computers group or some other group to which you want to install client software. Optionally, you can drag these computers into a new group that you create. See:

[Installing Windows clients with an Active Directory Group Policy Object \(GPO\)](#)

To create a GPO software distribution

1. On the Windows Taskbar, click **Start > All Programs > Administrative Tools > Group Policy Management**.
2. In the **Active Directory Users and Computers** window, in the console tree, right-click the domain, and then click **Active Directory Users and Computers**.
3. In the **Active Directory Users and Computers** window, select a target organizational unit (OU) under the appropriate domain.
You can also create a new OU for testing or other purposes. See Active Directory documentation by Microsoft for more information on how to create a new OU.
4. In the **Group Policy Management** window, in the console tree, right-click the organizational unit that you chose or created, and then click **Create and Link a GPO Here**.
You may need to refresh the domain to see a new OU.
5. In the **New GPO** dialog box, in the Name box, type a name for your GPO, and then click **OK**.
6. In the right pane, right-click the GPO that you created, and then click **Edit**.

-
7. In the **Group Policy Object Editor** window, in the left pane, under **Computer Configuration**, expand **Software Settings**.
 8. Right-click **Software installation**, and then click **New > Package**.
 9. In the **Open** dialog box, type the Universal Naming Convention (UNC) path that points to and contains the MSI package.
Use the format as shown in the following example:
`\\server_name\SharedDir\Sep.msi`
 10. Click **Open**.
 11. In the **Deploy Software** dialog box, click **Assigned**, and then click **OK**.
The package appears in the right pane of the Group Policy Object Editor window if you select Software Installation.

To configure administrative templates for the software package

1. To configure administrative templates for the software package, in the **Group Policy Object Editor** window, in the console tree, display and enable the following settings:
 - **Computer Configuration > Administrative Templates > System > Logon > Always wait for the network at computer startup and logon**
 - **Computer Configuration > Administrative Templates > System > Group Policy > Software Installation policy processing**
 - **User Configuration > Administrative Templates > Windows Components > Windows Installer > Always install with elevated privileges**

NOTE

If you enabled User Account Control (UAC) on the client computers, you must also enable **Computer Configuration > Administrative Templates > Windows Components > Windows Installer > Always install with elevated privileges** to install Symantec client software with a GPO. You set these options to allow all Windows users to install Symantec client software.

2. Close the Group Policy Object Editor window.
3. In the **Group Policy Management** window, in the left pane, right-click the GPO that you edited, and then click **Enforced**.
4. In the right pane, under **Security Filtering**, click **Add**.
5. In the dialog box, under **Enter the object name to select**, type `Domain Computers`, and then click **OK**.

Adding computers to an organizational unit to install software

You can add computers to an organizational unit to which Symantec Endpoint Protection installs by GPO. When the computers restart, the client software installation process begins. When users log on to the computers, the client software installation process completes. The group policy update, however, is not instantaneous, so it may take time for this policy to propagate. The following process contains the commands that you can run on the client computers to update the policy on demand. See:

[Installing Windows clients with an Active Directory Group Policy Object \(GPO\)](#)

To add computers to the organizational unit to install software

1. On the Windows Taskbar, click **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
2. In the **Active Directory Users and Computers** window, in the console tree, locate one or more computers to add to the organizational unit that you chose for GPO installation.
Computers first appear in the **Computers** organizational unit.
3. Drag and drop the computers into the organization unit that you chose or created for the installation.
4. Close the **Active Directory Users and Computers** window.

To update the GPO on demand on the client computers

1. Open a command prompt on the client computers.
2. Type `gpupdate`, and then press **Enter**.
When complete, the command prompt window displays a message to let you know the policy update completed successfully. If an error message displays, follow the on-screen instructions for more information.
3. Close the command prompt window.

Copying a Sylink.xml file to make a managed installation package

When you install Symantec Endpoint Protection Manager, it creates a file named Sylink.xml for each client group. Symantec Endpoint Protection clients read the contents of this file to know which management server manages the client. If you install the client from the installation file you get from Symantec, you install unmanaged clients. However, you can copy the Sylink.xml file to this folder before installation to install managed clients.

NOTE

Packages that are exported with the Symantec Endpoint Protection Manager console are managed and already include a Sylink.xml file. To export a new managed package that you can deploy with a Group Policy Object, use the Client Deployment Wizard. Click **Save Package**, and check **Separate Files (required for .MSI)** when prompted. See:

[Installing Symantec Endpoint Protection clients with Save Package](#)

To copy a Sylink.xml file to the product installation files to make a managed installation package

1. From Symantec Endpoint Protection Manager, export the Sylink.xml file from the correct client group and copy it to your computer.

NOTE

You should create at least one new group with the management console before you export the Sylink.xml file. If you do not, the clients appear in the Default group.

For more information, see:

- [Adding a group](#)
 - [Exporting the client-server communications file \(Sylink.xml\) manually](#)
2. Copy the installation folder from the installation file you download to a folder on your computer. The folder `SEP` contains the 32-bit client, and the folder `SEPx64` contains the 64-bit client.

You can also use the installation folder for an unmanaged client package that you previously exported as separate files.
 3. Copy Sylink.xml to the installation folder. Replace the existing Sylink.xml file when prompted.

Uninstalling client software with an Active Directory Group Policy Object

You can uninstall the client software that you installed with Active Directory. See:

[Uninstalling the Symantec Endpoint Protection client for Windows](#)

To uninstall client software with an Active Directory Group Policy Object

1. On the Windows Taskbar, click **Start > All Programs > Administrative Tools > Group Policy Management**.

The version of Windows that you use may display **Programs** instead of **All Programs** in the **Start** menu.

2. In the **Group Policy Management** window, in the console tree, expand the domain, expand **Computer Configuration**, expand **Software Settings**, right-click **Software Installation**, and then click **Properties**.
3. On the **Advanced** tab, check **Uninstall this application when it falls out of the scope of management**, and then click **OK**.
4. In the right pane, right-click the software package, and then click **Remove**.
5. In the **Remove Software** dialog box, check **Immediately uninstall the software from users and computers**, and then click **OK**.
6. Close the **Group Policy Object Editor** window, and then close the **Group Policy Management** window.

The software uninstalls when the client computers are restarted.

Quick Start Guide for Symantec™ Endpoint Protection for Amazon Web Services

Usage instructions and best practices for Symantec Endpoint Protection Manager on Amazon Web Services (AWS)

When you log on to Symantec Endpoint Protection Manager Amazon Machine Image (AMI) on Amazon Web Services for the first time, you should be aware of possible issues.

Table 234: Possible to Symantec Endpoint Protection Manager Amazon Machine Image (AMI) issues

Item	Description
Initial logon credentials	When you connect to the instance for the first time, Symantec Endpoint Protection Manager opens automatically and then prompts you to change the password.
LiveUpdate launches after initial logon	When Symantec Endpoint Protection Manager LiveUpdate launches for the first time, it downloads more content than during subsequent LiveUpdate sessions. As a result, the responsiveness of the instance slows down until LiveUpdate completes. This behavior is expected, and only occurs on this initial launch. LiveUpdate launches five minutes after your initial logon to Symantec Endpoint Protection Manager.
Client does not appear immediately in Symantec Endpoint Protection Manager	You may notice that the client that is preinstalled on the instance does not immediately display on the Home tab in Symantec Endpoint Protection Manager. This behavior is expected. After the heartbeat into Symantec Endpoint Protection Manager completes, the client appears on the Home tab.
Update the email address for admin	You must change the default email address for admin in Symantec Endpoint Protection Manager. By default, the email address is a@b.com. You can easily change this email address after you log on to Symantec Endpoint Protection Manager in the Admin pane, under Administrators > Edit the administrator . Since password recovery for Symantec Endpoint Protection Manager requires a valid email address, you should perform this task the first time you log on.
Update the database password	In version 14 or later, you can change the database password for Symantec Endpoint Protection Manager. You should change this password the first time you log on. See: Changing the password for an administrator account or the embedded database
Remote push deployment (optional)	Symantec Endpoint Protection Manager push deployment makes use of the ICMP ping protocol to look up the IP address of an instance on the network. You must explicitly add the ICMP Echo Request ingress rule on client instance candidates in order for them to be visible on the Symantec Endpoint Protection Manager Client Deployment Wizard. To successfully deploy the client package from Symantec Endpoint Protection Manager to the client instances, you must enable TCP port 445 on the client instances. See the section Security Groups for more information.

Item	Description
Security Groups	The following tables demonstrate recommended security group firewall rules for AMI instances running Symantec Endpoint Protection: For information on how to work with client instances, see: Amazon EC2 Security Groups for Windows Instances

Table 235: Incoming security group settings for Symantec Endpoint Protection instances

Type / Protocol	Applies to	Port number	Source	Purpose
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8014 443*	0.0.0.0/0	Used for HTTP communication between Symantec Endpoint Protection Manager and the Symantec Endpoint Protection clients. * = Used for the optional HTTPS configuration.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8443	0.0.0.0/0	Used for HTTPS communication between a remote management console and Symantec Endpoint Protection Manager. All logon information and administrative communication takes place using this secure port.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8444	0.0.0.0/0	Used by the Symantec Endpoint Protection Manager web services.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8445	0.0.0.0/0	Used for HTTPS communication for the reporting console.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	8765	0.0.0.0/0	Used for Tomcat shutdown.
Custom TCP Rule / TCP	Symantec Endpoint Protection Manager	9090	0.0.0.0/0	Used for the initial logon communication between a remote management console and Symantec Endpoint Protection Manager to display the logon screen.
Custom TCP Rule / TCP	Symantec Endpoint Protection client	445	0.0.0.0/0	Used for remote deployment of installation packages from Symantec Endpoint Protection Manager.
Custom ICMP Rule / Echo request	Symantec Endpoint Protection client	N/A	0.0.0.0/0	Used by Remote Push to look up the IP address of an Symantec Endpoint Protection client instance on the network.
RDP / TCP	Symantec Endpoint Protection Manager, Symantec Endpoint Protection client	3389	0.0.0.0/0	Used to remotely connect to the instance.

Table 236: Outgoing security group settings for Symantec Endpoint Protection instances

Type / Protocol	Applies to	Port number	Destination
All traffic / All	Symantec Endpoint Protection Manager Symantec Endpoint Protection client	All	0.0.0.0/0

Requirements to use Symantec Endpoint Protection Manager on Amazon Web Services

Amazon Web Services (AWS) account holders can subscribe to Symantec Endpoint Protection Manager on an Amazon Machine Image (AMI) or Amazon's Elastic Compute Cloud (EC2).

Table 237: Prerequisites, supported platforms, and instances to run the Symantec Endpoint Protection Manager AMI

Requirement	Details
Prerequisites	The prerequisites to use Symantec Endpoint Protection Manager AMI for Amazon EC2 are as follows: - You must have an AWS Marketplace account. To create an account or to access an existing account, go to: https://aws.amazon.com/marketplace - If you use the Bring Your Own License (BYOL) option, you must have a valid license for Symantec Endpoint Protection. To review your licensing status, log on to the Broadcom Support Portal and go to: Broadcom Download Center Alternately, you can contact support for non-technical questions about your license: Symantec customer support
Supported Platforms and Instances	Symantec Endpoint Protection Manager AMI for Amazon EC2 (BYOL and Paid) includes support for: - Symantec Endpoint Protection Manager, version 14 MP1 or later - Windows Server 2012 R2 or later Symantec Endpoint Protection Manager AMI supports the following Amazon EC2 instances of Windows Server 2012 on the AWS Marketplace: 10 client tier: m4.large (2x CPU, 8 GB RAM, EBS disk) 100 client tier: m4.xlarge (4x CPU, 16 GB RAM, EBS disk) 250 client tier: m4.2xlarge (8x CPU, 32 GB RAM, EBS disk) 500 client tier: c4.2xlarge (8x CPU, 15 GB RAM, EBS disk)

Additional reference

For information on using Amazon EC2 and Symantec Endpoint Protection AMI, see:

[Getting Started with AWS](#)

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The check mark in a Circle design is the registered trademark of NortonLifeLock Inc. and is used under license therefrom.

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b) (3), as applicable, or their successors.

Copyright © 2005–2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

